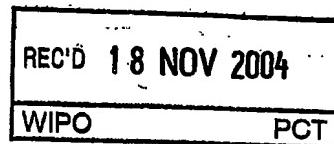


29.9.2004

日本国特許庁  
JAPAN PATENT OFFICE



別紙添付の書類に記載されている事項は下記の出願書類に記載されている事項と同一であることを証明する。

This is to certify that the annexed is a true copy of the following application as filed with this Office.

出願年月日 Date of Application: 2003年11月 7日

出願番号 Application Number: 特願2003-378574

[ST. 10/C]: [JP2003-378574]

出願人 Applicant(s): 松下電器産業株式会社

Best Available Copy

CERTIFIED COPY OF  
PRIORITY DOCUMENT

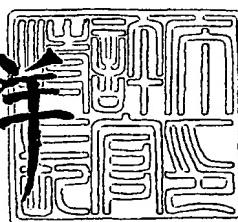
PRIORITY DOCUMENT  
SUBMITTED OR TRANSMITTED IN  
COMPLIANCE WITH  
RULE 17.1(a) OR (b)

2004年11月 5日

特許庁長官  
Commissioner,  
Japan Patent Office

小川

洋



【書類名】 特許願  
【整理番号】 2048150034  
【あて先】 特許庁長官殿  
【国際特許分類】 G06F 12/14  
H04N 5/7617  
H04N 5/915  
H04N 7/16

【発明者】  
【住所又は居所】 大阪府門真市大字門真1006番地 松下電器産業株式会社内  
【氏名】 東 吾紀男

【発明者】  
【住所又は居所】 大阪府門真市大字門真1006番地 松下電器産業株式会社内  
【氏名】 岡本 隆一

【特許出願人】  
【識別番号】 000005821  
【氏名又は名称】 松下電器産業株式会社

【代理人】  
【識別番号】 100109210  
【弁理士】  
【氏名又は名称】 新居 広守

【手数料の表示】  
【予納台帳番号】 049515  
【納付金額】 21,000円

【提出物件の目録】  
【物件名】 特許請求の範囲 1  
【物件名】 明細書 1  
【物件名】 図面 1  
【物件名】 要約書 1  
【包括委任状番号】 0213583

**【書類名】特許請求の範囲****【請求項 1】**

コンテンツを配信するコンテンツ配信サーバと、前記コンテンツの利用をセキュアに制御する端末装置と、から構成されるコンテンツ利用制御システムであって、

前記コンテンツ配信サーバは、

時刻情報を前記コンテンツに付加する時刻情報付加部と、

前記時刻情報を用いて、前記コンテンツの特定部分の利用を制御するための利用制御情報を、前記コンテンツとは別データとして生成する利用制御情報生成部と、

前記時刻情報を前記コンテンツにセキュアにバインドする時刻情報バインド部と、  
を備え、

前記端末装置は、

前記コンテンツを利用するコンテンツ利用部と、

前記コンテンツに付加されたセキュアな前記時刻情報と前記利用制御情報を用いて、  
前記コンテンツ利用部での前記コンテンツの利用をセキュアに制御するコンテンツ利用制御部と、

を備えることを特徴とするコンテンツ利用制御システム。

**【請求項 2】**

前記利用制御情報は、前記コンテンツの特殊再生を禁止する  
ことを特徴とする請求項 1 記載のコンテンツ利用制御システム。

**【請求項 3】**

前記利用制御情報は、前記コンテンツのプレビューを許可する  
ことを特徴とする請求項 1 記載のコンテンツ利用制御システム。

**【請求項 4】**

前記利用制御情報は、前記コンテンツの利用許可を与えるライセンスに設定される  
ことを特徴とする請求項 1 記載のコンテンツ利用制御システム。

**【請求項 5】**

前記利用制御情報は、デジタル放送のECM (Entitlement Control  
Message) に設定される  
ことを特徴とする請求項 1 記載のコンテンツ利用制御システム。

**【請求項 6】**

前記利用制御情報は、許可された利用または操作の種別を含む  
ことを特徴とする請求項 1 記載のコンテンツ利用制御システム。

**【請求項 7】**

前記利用制御情報は、特定の利用または操作が許可されるまでの回数または時間に関する  
制限を含む  
ことを特徴とする請求項 1 記載のコンテンツ利用制御システム。

**【請求項 8】**

前記利用制御情報は、許可された利用または操作の回数または時間に関する制限を含む  
ことを特徴とする請求項 1 記載のコンテンツ利用制御システム。

**【請求項 9】**

前記時刻情報は、MPEG-2 Systems のPES パケットに設定されたPTS  
(Presentation Time Stamp) である  
ことを特徴とする請求項 1 記載のコンテンツ利用制御システム。

**【請求項 10】**

前記コンテンツ利用制御部は、前記利用制御情報を未取得である場合、前記コンテンツの通常利用のみを許可する

ことを特徴とする請求項 1 記載のコンテンツ利用制御システム。

**【請求項 11】**

前記コンテンツ利用制御部は、前記利用制御情報を未取得である場合、前記コンテンツの特殊再生を禁止する

ことを特徴とする請求項 2 記載のコンテンツ利用制御システム。

【請求項 12】

前記コンテンツ利用制御部は、前記利用制御情報を未取得である場合、前記コンテンツのプレビューを禁止する

ことを特徴とする請求項 3 記載のコンテンツ利用制御システム。

【請求項 13】

前記端末装置は、少なくとも前記コンテンツの視聴箇所を含む視聴履歴を記録する視聴履歴記録部をさらに備え、

前記コンテンツ利用制御部は、前記利用制御情報に加え、さらに前記視聴履歴を用いて前記コンテンツ利用部での前記コンテンツの利用をセキュアに制御する

ことを特徴とする請求項 1 記載のコンテンツ利用制御システム。

【請求項 14】

前記コンテンツのリアルタイム視聴時と蓄積視聴時とで、前記コンテンツ利用制御部によって利用制御される前記コンテンツの箇所が異なる

ことを特徴とする請求項 1 記載のコンテンツ利用制御システム。

【書類名】明細書

【発明の名称】コンテンツ利用制御システム

【技術分野】

【0001】

本発明は、通信や放送を用いて、サーバ装置から映像、音楽などのデジタルコンテンツを配信し、ユーザが端末装置でデジタルコンテンツを利用するシステムに関し、特に、端末装置におけるデジタルコンテンツの特定部分について、タイムスキップや早送りなどの特殊再生を、事業者の意図に従って確実に制御することが可能なシステムに関する。

【背景技術】

【0002】

近年、音楽、映像、ゲームなどのデジタルコンテンツ（以下、コンテンツと記述）を、インターネットなどの通信や、デジタル放送、CATV（Cable Television）などを通じて、サーバ装置から端末装置に配信し、端末装置においてコンテンツを利用することが可能なコンテンツ配信サービスが実用化段階に入っている。このコンテンツ配信サービスに用いられる一般的なシステムでは、コンテンツの著作権を保護し、悪意あるユーザなどによるコンテンツの不正利用を防止するため、著作権保護技術が用いられる。著作権保護技術とは、具体的には、暗号技術や認証技術などを用いて、ユーザがコンテンツを再生したり、記録メディアにコピーしたりといったようなコンテンツの利用を、セキュアに制御する技術である。著作権保護技術を用いることにより、コンテンツプロバイダやサービスプロバイダなどの事業者が、ユーザの端末装置におけるコンテンツ利用をセキュアに制御することが可能となる。

【0003】

ところで、近年、HDD（Hard Disk Drive）などの大容量蓄積手段を有する端末装置において、配信されたコンテンツを一旦端末装置に蓄積し、ユーザが好きなときに好きなコンテンツを視聴するという、ユーザ利便性の高い利用形態が検討されている。日本におけるデジタル放送の規格化団体であるARIB（Association of Radio Industries and Businesses）においても、大容量蓄積機能を活用するデジタル放送方式として、サーバ型放送方式が規格化されている。サーバ型放送方式に関しては、ARIB STD-B25 4.1版が詳しい。

【0004】

しかしながら、このような蓄積機能を有する端末装置においては、コマーシャル（CM）を含んだコンテンツを一旦端末装置に蓄積し、タイムシフトによる視聴時にCM部分をスキップしたり、早送りしたりすることにより、ユーザがCMを視聴しないという事態が発生しうる。その結果として、事業者にとってCM効果が小さくなり、CM料金が低下するなどといったデメリットが発生する可能性がある。このような課題を解決する技術として、例えば、特許文献1には、サーバ装置でコンテンツのCM部分の前後にCMスキップ禁止信号、または、CMスキップ禁止解除信号を埋め込んでおくことにより、端末装置においてCMスキップの制御を行うシステムが、コンテンツ利用制御システムの一例として記載されている。

【0005】

このように、従来のコンテンツ利用制御システムでは、コンテンツのCM部分など、コンテンツ提供者側で特殊再生を禁止したい部分に、その旨を示す制御情報を埋め込んでおくことによって、事業者の意図に反したユーザのコンテンツ利用を防止することができるようになっている。

【特許文献1】特開2002-290878号公報

【発明の開示】

【発明が解決しようとする課題】

【0006】

しかしながら、従来のコンテンツ利用制御システムでは、CM部分の特殊再生を防止するため、コンテンツにCM視聴を制御するための制御情報を埋め込む必要がある。通常、

コンテンツをデジタル符号化するエンコーダには、コンテンツのCM部分を識別する機能はもちろんのこと、CM視聴制御のための情報を挿入する機能ですら有していないのが一般的である。よって、CM視聴を制御可能なコンテンツを生成するためには、専用のエンコーダが必要であり、その結果、事業者のコスト負担が大きくなるという課題があった。

#### 【0007】

本発明は、こうした従来の問題点を解決するものであり、コンテンツに制御情報を追加することなく、端末装置でのコンテンツのCM部分などのコンテンツの特定部分の利用制御をセキュアに実現することにより、低廉なコストで事業者の意図に反するユーザのコンテンツ利用を防止することが可能なコンテンツ利用制御システムを提供することを目的としている。

#### 【課題を解決するための手段】

#### 【0008】

上記目的を達成するために、本発明に関わるコンテンツ利用制御システムは、コンテンツを配信するコンテンツ配信サーバと、前記コンテンツの利用をセキュアに制御する端末装置とから構成されるコンテンツ利用制御システムであって、前記コンテンツ配信サーバは、時刻情報を前記コンテンツに付加する時刻情報付加部と、前記時刻情報を用いて、前記コンテンツの特定部分の利用を制御するための利用制御情報を、前記コンテンツとは別データとして生成する利用制御情報生成部と、前記時刻情報を前記コンテンツにセキュアにバインドする時刻情報バインド部とを備え、前記端末装置は、前記コンテンツを利用するコンテンツ利用部と、前記コンテンツに付加されたセキュアな前記時刻情報と、前記利用制御情報を用いて、前記コンテンツ利用部での前記コンテンツの利用をセキュアに制御するコンテンツ利用制御部とを備えることを特徴とする。

#### 【0009】

本構成によって、コンテンツに利用制御のための特別な情報を挿入することなく、コンテンツの特定部分の利用をセキュアに制御することが可能となる。

#### 【発明の効果】

#### 【0010】

本発明によれば、CMの視聴を制御するための制御情報をコンテンツ本体に埋め込むことなく、コンテンツに既存のセキュアな時刻情報を用いてセキュアにユーザのCM視聴を制御することができるため、一般的なエンコーダで生成したコンテンツを適用することができ、事業者のコスト負担を軽減することが可能となる。

#### 【発明を実施するための最良の形態】

#### 【0011】

以下、本発明における実施の形態について、図面を用いて詳細に説明する。

図1は、本発明における実施の形態に関するコンテンツ利用制御システム1の全体の概略構成を示す図である。

このコンテンツ利用制御システム1は、ネットワークなどを通じて配信センター（すなわち、サービスプロバイダ）から配信される暗号化コンテンツを、ユーザが端末装置において利用する際に、セキュアに再生制御を行うシステムであって、コンテンツやコンテンツの利用許諾を与えるライセンスなどを配信する配信センター101と、コンテンツを利用する端末装置102a～102cと、これらを相互に接続するネットワーク103とから構成されている。

#### 【0012】

配信センター101は、ユーザが所有するコンテンツを利用する権利（利用条件）の管理や、コンテンツのライセンスを生成し、端末装置102a～102cに配信を行う権利管理サーバ101aと、端末装置102a～102cにコンテンツを配信するコンテンツ配信サーバ101bと、ユーザに対して課金を行うための課金サーバ101cと、ネットワーク103を通じて端末装置102a～102cに各種サービスを提供するためのウェブ画面を送信するウェブサーバ101dとから構成されている。

#### 【0013】

権利管理サーバ101aは、ユーザが所有するコンテンツの利用条件を管理し、ユーザに暗号化されたコンテンツを復号するためのライセンスを付与するサーバ装置である。具体的には、権利管理サーバ101aは、ユーザ毎、あるいは、端末装置102a～102c毎に、それぞれが所有するコンテンツの利用条件を管理しておき、ユーザからの要求に基づき、インターネットなどのネットワーク103を通じて、ライセンスを端末装置102a～102cに配信する。また、デジタル放送やブロードバンドインターネットにおいて、push型の放送形態のコンテンツを配信する場合は、コンテンツとともにライセンスを配信するため、生成したライセンスをコンテンツ配信サーバ101bに送信する。

#### 【0014】

なお、ライセンスは、暗号化コンテンツを復号するための暗号鍵と、コンテンツの利用期限や利用回数などの利用条件などから構成される。ライセンスのデータ構造の例については、後で図を用いて詳細に説明する。

また、ライセンスなどのセキュリティを確保すべきデータを、ネットワーク103を通じて、配信センター101と端末装置102a～102cとの間で送受信する場合には、SSL (Secure Socket Layer) やTLS (Transport Layer Security) などの安全な認証チャネル (Secure Authenticated Channel、以下、SACと記述) を確立し、データの送受信を行う。

#### 【0015】

コンテンツ配信サーバ101bは、ネットワーク103を通じて端末装置102a～102cにコンテンツを配信するためのサーバ装置であり、専用ハードウェアやワープロセッショニングなどにより実現される。具体的には、コンテンツ配信サーバ101bは、MPEG-2やMPEG-4などの圧縮方式によりデジタル圧縮され、必要に応じて、AES (Advanced Encryption Standard) やTriple DES (Data Encryption Standard) などの共通鍵暗号アルゴリズムなどにより暗号化した上で、暗号化コンテンツをストリーミング配信、あるいは、ダウンロード配信する。

#### 【0016】

特に、BS (Broadcasting Satellite) デジタル放送、CS (Communication Satellite) デジタル放送、地上波デジタル放送におけるサーバ型放送方式では、MPEG-2やMPEG-4のコンテンツ (Elementary Stream、以下、ESと記述) を、PES (Packetized Elementary Stream) / TS (Transport Stream) により多重化された、リアルタイム視聴と蓄積視聴の共用が可能なストリーム型コンテンツを配信する方式が規格化されており、サーバ型放送方式タイプIと称される。

#### 【0017】

ここで、図2を用いて、サーバ型放送方式タイプIをベースとしたコンテンツ配信における暗号鍵スキームについて簡単に説明する。

図2において、コンテンツ・暗号鍵を配信する送信側と、コンテンツ・暗号鍵を受信する受信側に分けて説明する。まず、送信側では、コンテンツはスクランブル鍵Ks201と呼ばれる暗号鍵によって暗号化(202)、すなわち、スクランブルされ、受信側に送信される。コンテンツのスクランブルについては、MPEG-2 TSのパケット単位で、TSパケットのペイロード部をスクランブルする。また、スクランブル鍵Ks201は、不正受信に対するセキュリティ向上のため、数秒おきに変更される時変鍵である。

#### 【0018】

また、コンテンツをスクランブルするスクランブル鍵Ks201は、ワーク鍵Kw203を用いて暗号化(204)され、受信側に送信される。ワーク鍵Kw203は、従来の一般的な限定受信方式で用いられている放送事業体毎の契約単位、グループ単位に割り当てられる暗号鍵であり、ワーク鍵Kw203自体のセキュリティを確保するため、数ヶ月～数年の期間で更新されるのが一般的である。少なくともスクランブル鍵Ks201を含

み、コンテンツに関する情報を送信するためのデータ構造は、ECM (Entitlement Control Message) と呼ばれ、MPEG-2 Systems のプライベートセクションとして構成される。ワーク鍵Kw203で暗号化されたECMは、ECM-Kwと呼ばれ、放送コンテンツのリアルタイム視聴において利用する。

#### 【0019】

また、コンテンツをスクランブルするスクランブル鍵Ks201は、コンテンツ鍵Kc205を用いて暗号化(204)され、受信側に送信される。コンテンツ鍵Kw205は、コンテンツ単位に割り当てられる暗号鍵であり、ECM-Kwと同様、MPEG-2 Systems のプライベートセクションとして構成される。少なくともスクランブル鍵Ks201を含むECMを、コンテンツ鍵Kc205で暗号化したものをECM-Kcと呼び、放送コンテンツの蓄積視聴において利用する。

#### 【0020】

さらに、コンテンツ鍵Kc205はワーク鍵Kw203で暗号化され、受信側に送信される。少なくともコンテンツ鍵Kc205を含み、ワーク鍵Kw203で暗号化されたECMをKc配信用ECMと呼び、放送コンテンツの蓄積視聴において利用する。Kc配信用ECMは、ECM-Kw、および、ECM-Kcと同様に、MPEG-2 Systems のプライベートセクションとして構成されるものである。

#### 【0021】

なお、ECM-Kw、ECM-Kc、Kc配信用ECMのデータ構造の例については、後で図を用いて詳細に説明する。

以上のように生成された暗号化コンテンツ、ECM-Kw、ECM-Kc、および、Kc配信用ECMは、MPEG-2 TSパケット化され、必要に応じてPSI (Program Specific Information) / SI (Service Information)などのデータと多重化(207)された後、受信側に送信される。

#### 【0022】

一方、受信側では、暗号化コンテンツ、ECM-Kw、ECM-Kc、および、Kc配信用ECMが多重化されたMPEG-2 TSパケットを受信し、これらを分離(210)して、暗号化コンテンツ、ECM-Kw、ECM-Kc、Kc配信用ECMを取得する。

リアルタイム視聴時には、ECM-Kwを取得して、あらかじめ受信側が保持しているワーク鍵Kw203によりECM-Kwを復号(212)して、スクランブル鍵Ks201を取得する。これにより、暗号化コンテンツを復号(213)して、コンテンツを利用することが可能となる。なお、ECM-Kwは、リアルタイム視聴時のみで使用されるため、図示しない蓄積部に記録する必要はない。

#### 【0023】

一方、蓄積視聴時には、図示しない蓄積部に記録された暗号化コンテンツ、ECM-Kc、Kc配信用ECMを読み出す。ワーク鍵Kw203によりKc配信用ECMを復号(214)して、コンテンツ鍵Kc205を取得する。これによりコンテンツ鍵Kc205によりECM-Kcを復号(212)し、暗号化コンテンツを復号(213)して、コンテンツを利用することが可能となる。

#### 【0024】

なお、ARIB STD-B25 4.1版では、上記説明に加えて、送信側と受信側とで、ワーク鍵Kw203を共有するための方法について記載されているが、本発明における実施の形態では、送信側と受信側との間でSACを確立し、通信によりワーク鍵Kw203を共有する場合について説明する。もちろん、ARIB STD-B25 4.1版に記載されているように、EMM (Entitlement Management Message) と呼ばれるデータ構造を利用して、放送を用いてワーク鍵Kw203を配信することによって、送信側と受信側とでワーク鍵Kw203を共有するようにしても良い。この場合、EMMが盗聴されることを防止するため、マスタ鍵と呼ばれる受信端末毎に固有の鍵で暗号化されて配信される。このマスタ鍵は、送信側と受信側で予め共有さ

れる暗号鍵であり、受信側では端末装置102のセキュアな場所で管理されるか、セキュリティモジュールと呼ばれる耐タンパ性の高いモジュールにあらかじめ書き込まれて出荷され、セキュリティモジュールを端末装置102に挿入して用いられる。

#### 【0025】

また、ここでは、ワーク鍵Kw203により暗号化されたKc配信用ECMを蓄積部（図2に図示せず）に蓄積するにあたり、簡単のため、暗号変換を行わずにそのまま蓄積する場合の例を示したが、ワーク鍵Kw203の定期的または不定期の更新に備えるため、受信側があらかじめ保持する暗号鍵、例えば、複数の端末装置102であらかじめ共有している暗号鍵（グループ鍵）や端末装置102に固有のマスタ鍵を用いて、Kc配信用ECMの暗号変換を行うようにしても良い。

#### 【0026】

以上、図2を用いて、サーバ型放送方式タイプIをベースとした暗号鍵スキームについて説明した。以降、本発明における実施の形態では、図2で説明した暗号鍵スキームに基づくコンテンツ利用制御システムについての説明を行う。

また、コンテンツ配信サーバ101bは、端末装置102a～102cでのコンテンツの再生制御を行うため、コンテンツのCM部分やプレビュー部分など、コンテンツにあらかじめ設定された属性情報に基づき、コンテンツの特定箇所の再生制御を行うための再生制御情報を生成して、ECMとともに端末装置102a～102cに配信する。

#### 【0027】

課金サーバ101cは、インターネットなどを通じて、コンテンツの利用条件などを購入する際に、オンラインでの課金を行うためのサーバ装置である。具体的には、課金サーバ101cは、クレジットカードを用いて課金、決済を行ったり、あらかじめ課金サーバ101cにユーザの銀行口座番号を登録しておき、ネットワーク103を経由して端末装置102a～102cからアップロードされた購入の履歴などに基づき、課金、決済を行ったりする。

#### 【0028】

ウェブサーバ101dは、ユーザが端末装置102a～102cから各種サービスにアクセスするためのコンテンツ購入画面などを提供する。具体的には、ウェブサーバ101dは、インターネットを通じて、HTTPなどのプロトコルにより、HTML（HyperText Markup Language）やXML（Extensible Markup Language）などのスクリプト言語で記述されたウェブページを提供したり、デジタル放送において、BML（Broadcasting Markup Language）で記述されたページを提供したりする。

#### 【0029】

LAN101nは、配信センター101において、権利管理サーバ101aと、コンテンツ配信サーバ101bと、ウェブサーバ101dと、課金サーバ101cとを相互に接続するためのネットワークである。例えば、IEEE802.3などの有線ネットワークや、IEEE802.11bなどの無線ネットワークを用いて実現することができる。

ネットワーク103は、配信センター101と端末装置102a～102cとを相互に接続するネットワークである。例えば、ネットワーク103は、インターネットなどの通信ネットワークや、デジタル放送、あるいは、これらが複合したネットワークである。

#### 【0030】

端末装置102a～102cは、ネットワーク103と接続する機能を有し、ユーザがコンテンツをモニター画面などで利用したり、記録メディアにコンテンツを書き出したりするための端末装置である。具体的には、端末装置102a～102cは、デジタル放送を受信するためのSTB（Set Top Box）、デジタルTV、DVD（Digital Versatile Disc）レコーダ、HDDレコーダ、PC（Personal Computer）などのコンテンツ表示装置、レコーダ、あるいは、これらの複合機器である。

#### 【0031】

このようなコンテンツ利用制御システム1において、デジタル放送やブロードバンドインターネットなどのネットワーク103を通じてコンテンツやライセンスが配信され、端末装置102a～102cにおいてライセンス、および、再生制御情報に基づきコンテンツを視聴する処理を、図3～図32の図面を用いて詳細に説明する。但し、以下では、端末装置102a～102cについては、端末装置102aをその代表とし、端末装置102として説明する。

### 【0032】

図3は、図1に示される配信センター101における権利管理サーバ101aの詳細な構成を示す機能プロック図である。

権利管理サーバ101aは、大きく分けて、HDDなどに格納されたデータファイルなどによって実現されるデータベース部300と、システムLSIなどのハードウェアあるいはCPU、RAM、ROMなどをを利用して実行されるプログラムなどによって実現されるライセンス処理部310とから構成されている。

### 【0033】

データベース部300は、鍵情報DB301、ユーザ情報DB302、利用条件DB303、コンテンツ情報DB304とから構成されている。

鍵情報DB301は、ユーザが事業者（サービスプロバイダ）とサービスを契約することによって与えられるワーク鍵Kw203、および、コンテンツ毎に割り当てる蓄積視聴時のためにコンテンツ鍵Kc205を管理するデータベースであり、コンテンツ配信サーバ101bがECM-Kw、ECM-Kc、Kc配信用ECMを生成する際にワーク鍵Kw203、コンテンツ鍵Kc205を提供したり、端末装置102からワーク鍵Kw203を含むライセンスをリクエストされた際に、ユーザの契約（契約ID）に対応するワーク鍵Kw203を検索したりする場合に用いられる。

### 【0034】

具体的には、鍵情報DB301は、図4に示すように、契約ID401に対応するワーク鍵ID402とワーク鍵Kw203の組を管理するワーク鍵管理テーブル400を管理する。

例えば、図4では、契約ID401が「CONTRACT-ID-00001」に対応するワーク鍵ID402は「Kw-ID-00001」であり、ワーク鍵Kw203が「0x2340685345310911」であることを示している。ここで、契約ID401とは、事業者が提供するサービスに対する一種の契約形態を示し、例えば、スポーツに関するコンテンツを視聴できる「スポーツコンテンツパック」、映画コンテンツを視聴できる「映画コンテンツパック」などがあげられる。但し、契約ID毎にワーク鍵Kw203を割り当てるのではなく、サービスプロバイダ毎にワーク鍵Kw203を割り当て、契約ID401の識別をライセンス中に設定される利用条件で判別したり、ECMの項目として契約IDを含めるようにしたりすることも可能である。また、ワーク鍵ID402は、ECMを暗号化しているワーク鍵Kw203を特定するために用いられる情報である。

### 【0035】

また、鍵情報DB301は、図5に示すように、コンテンツ利用制御システム1においてコンテンツを一意に識別するコンテンツID501と、コンテンツID501に対応するコンテンツ鍵Kc205とからなるコンテンツ鍵管理テーブル500とを管理する。

例えば、コンテンツID501が「CONTENT-ID-00001」の暗号化コンテンツを復号するためのコンテンツ鍵Kc205が「0x1234567890abcd ef」であることを示している。

### 【0036】

ユーザ情報DB302は、ユーザに関する情報を管理するためのユーザ情報管理テーブルを有するデータベースであって、権利管理サーバ101aにアクセスする端末装置102と、利用条件DB303で管理される利用条件を所有するユーザとを関連付けるために用いられる。

具体的には、ユーザ情報DB302は、図6に示すユーザ情報管理テーブル600を有し、コンテンツ利用制御システム1内でユーザを一意に特定するためのユーザID601と、コンテンツ利用制御システム1内で端末装置102を一意に特定するための端末ID602とを管理している。

#### 【0037】

例えば、図6において、ユーザID601が「USER-ID-00001」であるユーザは、端末ID602が「TERMINAL-ID-00001」である端末装置102を所有していることを示している。また、ユーザID601が「USER-ID-00002」であるユーザは、端末ID602が「TERMINAL-ID-12345」、「TERMINAL-ID-54321」という2つの端末装置102を有しており、両方の端末装置102から権利管理サーバ101aにアクセス可能であることを示している。

#### 【0038】

なお、ユーザ情報DB302へのデータ登録は、ユーザによって、サービスプロバイダが提供するサービスを受けるために会員登録をする際に行なわれる。この会員登録処理は、ユーザがネットワーク103を通じてウェブサーバ101dが提供する会員登録画面により、配信センター101と端末装置102とがオンラインで行っても良いし、会員登録用の葉書を用いるなど、オフラインで行っても良い。会員登録処理では、まずサービスプロバイダがユーザに対してユーザID601を割り当てる。その後、ユーザが所有する端末装置102の端末ID602が、オンラインまたはオフラインによりサービスプロバイダに通知されるので、ユーザID601と端末ID602とが関連付けられて、ユーザ情報DB302のユーザ情報管理テーブル600に登録される。以上のような会員登録処理を行った結果、ユーザ情報DB302が構築される。

#### 【0039】

利用条件DB303は、ユーザ毎の事業者との契約に対する利用条件を管理するデータベースであって、端末装置102からのライセンス取得要求に対して、ユーザが所有する利用条件を満たすか否かを判定し、利用条件を満たす場合にライセンスを生成するために用いられる。

具体的には、利用条件DB303は、図7に示すように、コンテンツ利用制御システム1においてユーザを一意に識別し、利用条件の所有者を示すユーザID701と、ユーザID701に示されるユーザが所有する利用条件を識別するための利用条件ID702と、コンテンツ利用制御システム1においてユーザの契約形態を一意に識別する契約ID703と、契約ID703で示される契約の開始日時、終了日時を示す有効期間704と、契約ID703で示される契約形態に対応するライセンスの発行の残り回数を示す発行可能残回数705とからなる利用条件管理テーブル700を有する。

#### 【0040】

例えば、ユーザID701が「USER-ID-00001」であるユーザは、利用条件ID702が「URUs-ID-00001」なる利用条件を保持している。利用条件「URUs-ID-00001」は、ユーザが事業者と結んだ契約が、契約ID703に示される「CONTRACT-ID-00001」なる契約であり、有効期間704は「2002/12/31～2003/1/30」であり、ライセンスとして発行可能な回数が発行可能残回数705に示されている「1」回であることを示している。また、ユーザID701が「USER-ID-00002」であるユーザは、利用条件ID702が「URUs-ID-00002」と「URUs-ID-10011」という2つの利用条件を有している。このうち、利用条件「URUs-ID-00002」は、契約ID703が「CONTRACT-ID-13452」なる契約形態に対する利用条件であり、有効期間704が「2002/12/1～2002/12/31」、発行可能残回数705が「1」であるので、上記有効期間を有するライセンスを残り1回発行可能であることを示している。また、利用条件「URUs-ID-10011」は、コンテンツID703が「CONTRACT-ID-99999」なる契約形態に対する利用条件であり、有効期

間704は無制限（∞）であり、発行可能なライセンス数も無制限であることを示している。

#### 【0041】

コンテンツ情報DB304は、コンテンツ毎に設定するライセンス（後述するサプライセンス）を生成するために用いられる、コンテンツ毎の利用条件を格納するデータベースである。

具体的には、コンテンツ情報DB304は、図8に示すコンテンツ情報管理テーブル800を有し、コンテンツ利用制御システム1内でコンテンツを一意に特定するためのコンテンツID801と、コンテンツ利用制御システム1内でライセンスを一意に特定するためのライセンスID802と、ライセンスが有効である期間を示す有効期間803と、ライセンスを利用可能な回数を示す利用可能回数804とを管理している。

#### 【0042】

例えば、図8において、コンテンツID801が「CONTENT-ID-00001」であるコンテンツは、ライセンスID802が「LICENSE-ID-00001」、有効期間803が「2003/12/31～2004/1/30」、利用可能回数804が「∞（制限なし）」であることを示しており、これらの値がサプライセンスに設定される。

以上、図3～図8を用いて、データベース部3'00の各部についての詳細な説明を行った。

#### 【0043】

次に、ライセンス処理部310の各部についての詳細な説明を行う。ライセンス処理部310は、ライセンス発行部311、サーバ送受信部312とから構成されている。

ライセンス発行部311は、端末装置102からのライセンス発行要求に応じて、ユーザに対するライセンス（後述するメインライセンス）を生成するための部である。また、コンテンツ鍵Kc205をデジタル放送経由でコンテンツとともに端末装置102に送信するため、コンテンツ鍵Kc205を含むライセンス（後述するサプライセンス）を発行し、コンテンツ配信サーバ101bに送信する処理を行う。

#### 【0044】

具体的には、ライセンス発行部311は、端末装置102からのライセンス発行要求を受け、鍵情報DB301のワーク鍵管理テーブル400と、ユーザ情報DB302と、利用条件DB303とを利用し、ライセンス発行要求がユーザの利用条件を満たすか否かを判定した上で、ユーザの契約に対応するライセンスを生成する処理を行う。ユーザの契約に対して発行され、契約に対応する複数のコンテンツが利用可能なライセンスをメインライセンスと呼び、図2に示したワーク鍵Kw203を含む。

#### 【0045】

一方、コンテンツ配信サーバ101bに送信するライセンスは、单一コンテンツに対して発行されるライセンスであり、サプライセンスと呼ばれる。サプライセンスは図2に示したコンテンツ鍵Kc205を含み、ワーク鍵Kw203で暗号化される。また、サプライセンスは、コンテンツ配信サーバ101bでECMに設定され、端末装置102に送信される。よって、サプライセンスが設定されたコンテンツを利用するためには、サプライセンスを暗号化しているワーク鍵Kw203が設定されたメインライセンスを取得する必要がある。

#### 【0046】

サーバ送受信部312は、ネットワーク103を通じて、端末装置102と通信するための部である。

以上、権利管理サーバ101aの詳細な構成についての説明を行った。

ここで、ライセンス発行部311が生成するメインライセンス、および、サプライセンスについての構成を図9～図10を用いて詳細に説明する。

#### 【0047】

図9は、メインライセンスの構成の一例を示す図である。図9に示すメインライセンス

900は、メインライセンス900が利用を許諾するコンテンツの集合、すなわち、サブスクリプション（契約）の種類を識別する契約IDやメインライセンス900の有効期限（契約の有効期限）などを含むライセンスヘッダ901、コンテンツの再生や、記録メディアへのコピーなどに関する利用条件を示すアクションタグプロック902、暗号化されたコンテンツ鍵Kc205を復号するためのワーク鍵Kw203を含む暗号鍵タグプロック903、メインライセンス900の改ざんを検出するためのハッシュ値であるライセンスフッタ904とから構成されている。

#### 【0048】

ライセンスヘッダ901は、メインライセンス900を識別するためのライセンス識別子911、ユーザ毎またはシステム毎でメインライセンス900を一意に特定可能な識別子であるライセンスID912、メインライセンス900全体の長さを示すライセンスサイズ913、メインライセンス900が利用可能な期間を示すライセンス有効期間914から構成される。

#### 【0049】

アクションタグプロック902は、「再生」、「コピー」、「印刷」などの、コンテンツに対するユーザのアクションを特定するためのアクションID921と、コンテンツの再生、コピーなどを行う部に固有な利用条件を示す利用部固有条件922とから構成される。ここで、利用部固有条件922とは、端末装置102においてコンテンツを利用する機能を提供するコンテンツ利用部の種類や性能に依存する利用条件である。例えば、映画コンテンツの音声チャネルの指定（5.1chで再生可能か、2chで再生可能か）や、映像コンテンツの解像度、サイズの指定などが挙げられる。

#### 【0050】

暗号鍵タグプロック903は、ワーク鍵Kw203がバイナリ値で設定され、ECM-KwやKc配信用ECMなどのサプライセンスを含むECMを復号するために用いられる。

ライセンスフッタ904は、メインライセンス900をハードディスクなどの非セキュアな領域に蓄積する場合に、改ざんの検出を行い、その正当性を確保するためのものであって、メインライセンス900の内容が更新される度に、メインライセンス900の改ざんを防止したい箇所についてのハッシュ値を計算し、計算結果を管理する。このハッシュ値は、ハード的に耐タンパされたエリアで管理される必要がある。具体的なハッシュアルゴリズムとしては、SHA-1 (Secure Hash Algorithm. 1) や、SHA-256などを用いることができる。

#### 【0051】

一方、図10はサプライセンスの一例を示す図である。サプライセンス1000は、メインライセンス900と比較して、サプライセンス1000が利用を許諾する単一のコンテンツを指定するため、ライセンスヘッダ901にコンテンツID1014が設定できるようになっている。また、アクションタグプロック1002には、コンテンツの再生や、記録メディアへのコピーが可能な回数などの利用条件を示す回数カウンタ1022が存在している。また、暗号鍵タグプロック1003には、ECM-Kcを復号するためのコンテンツ鍵Kc205がバイナリ値で設定される。サプライセンス1000における他の項目については、メインライセンス900と同様であるので、ここでは説明を省略する。なお、メインライセンス900とサプライセンス1000で同一の項目がある場合は、サプライセンス1000に設定されている値を適用するものとするが、運用に応じて、どちらのライセンスを優先的に適用するかを決定しても良い。

#### 【0052】

以上、図9～図10を用いて、コンテンツ利用制御システム1におけるライセンスであるメインライセンス900およびサプライセンス1000について、その詳細な構成の説明を行ったことにより、ライセンス処理部310の各々の部についての詳細な説明を終了する。

次に、図11は、図1に示される配信センター101におけるコンテンツ配信サーバ1

01bの詳細な構成を示す機能ブロック図である。

**【0053】**

コンテンツ配信サーバ101bは、MPEG-2、MPEG-4などのコンテンツをMPEG-2 TSパケットの形式で出力する装置であって、コンテンツDB1101と、コンテンツ属性情報DB1102と、計時部1103と、時刻情報付加部1104と、コンテンツ符号化部1105と、再生制御情報生成部1106と、ECM生成部1107と、コンテンツ多重化部1108と、コンテンツ暗号化部1109と、コンテンツ送出部1110とから構成される。

**【0054】**

コンテンツDB1101は、コンテンツを蓄積するためのデータベースである。具体的には、コンテンツDB1101は、例えば、映画、ドキュメンタリーなどを蓄積するVC R (Video Cassette Recorder)などであったり、ライブ放送(生放送)時であれば、映像、音声を撮影するためのビデオカメラであったりする。

コンテンツ属性情報DB1102は、コンテンツ名称やコンテンツ中の構成内容など、コンテンツに関する種々の情報を蓄積するためのデータベースである。具体的には、コンテンツ属性情報DB1102は、図12に示すように、本コンテンツ利用制御システム内でコンテンツを一意に特定するためのコンテンツID1201と、コンテンツ名を示すコンテンツ名称1202と、コンテンツがPPV (Pay Per View)型のコンテンツである場合において、コンテンツ購入前の試聴を許可する区間を示すプレビュー可能区間1203と、コンテンツ中に含まれるCM部分を示すCM区間1204とを有するコンテンツ属性情報管理テーブル1200を備えている。

**【0055】**

例えば、コンテンツID1201が「CONTENT-ID-00001」であるコンテンツは、コンテンツ名称1202が「井上哲也NEWS23」であり、プレビュー可能区間1203はコンテンツの先頭からの相対値として「0分～10分」であり、CM区間1204はコンテンツの先頭からの相対値として、「5分～8分」、「20分～25分」、「40分～43分」という属性を有することを示している。また、コンテンツID1201が「CONTENT-ID-00002」である「プロダクトX」というコンテンツ名称1202のコンテンツに関しては、リアルタイム視聴時のプレビュー可能区間(0分～10分)と、蓄積視聴時のプレビュー可能区間(5分～10分、20分～30分、など)とが異なる属性を有しており、蓄積視聴の特徴を生かしたコンテンツ属性の設定がされている。また、CM区間1204に関しては、CMを含むコンテンツではないため、「ー(CM無し)」となっている。なお、プレビュー可能区間1203が設定されていないコンテンツに関しては、プレビューが許可されていないことを示し、CM区間1204が設定されていないコンテンツに関しては、CMが含まれていないコンテンツなので、コンテンツ内で特殊再生を禁止する部分が存在しないことを示している。

**【0056】**

計時部1103は、コンテンツ配信サーバ101b内での基準となる時刻を出力する部である。具体的には、計時部1103は、STC (System Time Clock)と呼ばれる27MHzの精度を有する42ビットの基準時刻を生成して、時刻情報付加部1104に供給する。

時刻情報付加部1104は、計時部1103から時刻情報を取得し、コンテンツ符号化部1105に対して時刻情報を付加する部である。具体的には、時刻情報付加部1104は、計時部1103からSTCの値を取得して、コンテンツ符号化部1105に対して、MPEG-2 Systemsの規約に従い、少なくとも700msの精度でPTS (Presentation Time Stamp)およびDTS (Decoding Time Stamp)のためのタイムスタンプを付与する。また、MPEG-2 Systemsの規約に従い、少なくとも100msの精度でPCR (Program Clock Reference)のためのタイムスタンプを付与する。

**【0057】**

なお、ここでは、計時部1103および時刻情報付加部1104は、次に説明するコンテンツ符号化部1105の外部に備える場合の例を示したが、コンテンツ符号化部1105の内部に備えるようにしても良い。

コンテンツ符号化部1105は、端末装置102に送出するコンテンツをコンテンツDB1101から読み出し、コンテンツをMPEG形式で符号化する部である。

#### 【0058】

具体的には、コンテンツ符号化部1105は、MPEGストリームを生成するリアルタイムエンコーダであって、上流システム（例えば、番組運行管理システムなど）の指示により、コンテンツDB1101から映像、音声などを読み出し、映像、音声、データなどのMPEG-2やMPEG-4のESを生成する。さらに、これらのESを含むPESパケットを生成し、最後にMPEG-2 TSパケット化して、コンテンツ多重化部1108に送出する。

#### 【0059】

ここで、図13を用いて、PESパケットの構成の概要について説明する。図13に示すPESパケット1300は、PESパケットの開始を示すコードであるPacket Start Code Prefix1300と、PESに含まれる音声、映像などのデータの種類を示すStream id1320と、PESパケット1300の長さを示すPES Packet Length1330と、オプションのPESヘッダであるOptional PES Header1340と、スタッフィングであるStuffing Bytes1350と、音声、映像などのデータ（ES）が設定されるPES Packet Data Bytes1360とから構成される。

#### 【0060】

また、図14は、TSパケットの構成の概要を示す図である。TSパケット1400は、TSパケット1400の開始を示すコードやTSパケットに設定されるデータの種類などを特定するためのPID(Packet ID)、TSパケットのペイロード（後述するTSP Payload1430）の暗号化の有無を示すフラグであるtransport\_scrambling\_controlなどが含まれるTSパケット1400のヘッダであるTSP Header1410と、オプション的に用いられ、時刻情報やプライベートデータなどが設定可能なAdaptation Field1420と、PESパケット1400や、PSI/SIなどが設定されるペイロードであるTSP Payload1430とから構成される。

#### 【0061】

なお、MPEG-2 SystemsのPESパケットやTSパケットについては、国際標準規格であるISO/IEC 13818-1が詳しい。

図13および図14で説明したPESパケット1300およびTSパケット1400を用いて、コンテンツ符号化部1105が設定する時刻情報について説明する。コンテンツ符号化部1105は、時刻情報付加部1104から取得した時刻情報、すなわちSTCの値を用いて、PESパケット1300を生成する際、Optional PES Header1340中の、Optional Fields1343の要素であるPTS1343a、DTS1343bをPESパケット1300に付加する。

#### 【0062】

PTS1343aは、当該PESパケット1300に含まれる映像、音声などを端末装置102a～102cにおいて表示する時刻を示す情報である。また、DTS1343bは、当該PESパケット1300に含まれる映像、音声などをデコードする時刻を示す情報である。

これらのPTS1343aおよびDTS1343bは、端末装置102a～102cにおいて、端末装置102a～102cが保持するSTCと一致する毎に、個々のPESパケットのデコード、表示を確実に行えるようにするために、適切なPESパケット1300に設定されるものである。

#### 【0063】

また、コンテンツ符号化部1105は、TSパケット1400を生成する際、時刻情報付加部1104から取得した時刻情報(STC)の値を用いて、TSパケット1400のAdaptation Field1420のOptional Fields1425内の要素であるPCR1425aを付加する。端末装置102a～102cは、このPCR1425aを用いて、複数のES(映像、音声、データなど)を同期させる際の基準となり、送信装置のSTCと同期した基準クロック(STC)を再生することが可能となる。

#### 【0064】

以下、図11に戻って、コンテンツ配信サーバ101bの構成についての説明を継続する。

再生制御情報生成部1106は、コンテンツの特定部分の再生を制御するための情報を生成する部である。具体的には、再生制御情報生成部1106は、コンテンツ配信サーバ101bから送出するコンテンツについて、コンテンツ属性情報DB1102が管理するコンテンツ属性情報管理テーブル1200から、対応するコンテンツのプレビュー可能区間1203およびCM区間1204を取得し、再生制御情報として、それぞれに対応するプレビュー制御情報、および、CMスキップ制御情報を生成する。この再生制御情報を、権利管理サーバ101aで生成されたサブライセンス1000に設定するため、サブライセンス1000に設定可能な形式である制御情報タグблокを生成し、制御情報タグblock中に再生制御情報を設定する。この制御情報タグblockのデータ構造を図15に示す。

#### 【0065】

図15に示す制御情報タグblock1500は、本タグblockが制御情報タグblock1500であることを示す制御情報タグ値1501と、制御情報タグblock1500のサイズを示す制御情報長1502と、プレビュー制御情報やCMスキップ制御情報などの再生制御情報を示す制御情報1503とから構成されている。

さらに、制御情報1503は、制御情報1503に含まれる再生制御情報の個数を示す制御情報個数1510と、再生制御内容を示す制御ID1511と、再生制御の期限を示す制御期限1512と、再生制御を行う回数を示す制御回数1513と、再生制御を行うコンテンツの特定箇所をコンテンツに附加された時刻情報を用いて指定する制御範囲1514とから構成されている。制御範囲1514は、再生制御を行うコンテンツの特定箇所を、制御開始時刻(1521、1523)と制御終了時刻(1522、1524)の組を用いて指定している。また、制御範囲1514に含まれる制御開始時刻と制御終了時刻の組は、複数個設定される可能性があるため、制御時刻個数1520として、制御範囲1514に設定された制御開始時刻と制御終了時刻の組の個数を示すようになっている。

#### 【0066】

このとき、コンテンツ属性情報管理テーブル1200のプレビュー可能区間1203およびCM区間1204は、コンテンツの先頭からの相対時刻となっているため、実際にコンテンツに附加される時刻情報(PTS1343a)を用いた値に変換する必要がある。PTS1343aは90KHzのクロック値であるため、コンテンツの先頭からの相対時刻を90000で除することによって、コンテンツの先頭からのPTS1343aに基づく相対時刻に変換することができる。さらに、コンテンツの先頭のPTS1343aの値を取得することで、コンテンツに附加されたPTS1343aを用いて、プレビュー可能区間およびCMスキップ制御区間を表現することができる。制御範囲1514に設定する制御開始時刻と制御終了時刻の組は、このようにPTS1343aを用いた時刻情報として設定される。

#### 【0067】

ところで、制御範囲1514を含む再生制御情報は、サブライセンス1000に設定され、さらにECMに設定されて、コンテンツ配信サーバ101bから端末装置102に配信される。このとき、端末装置102での連続するコンテンツのシームレスな再生を実現するため、ECMはコンテンツが実際に開始する数秒前から送出される。このため、再生

制御情報をコンテンツの符号化、送出前に生成する必要があり、再生制御情報の生成にあたってはコンテンツの先頭のPTS1343aを計算により求める必要がある。図16は、コンテンツの先頭のPTS1343aを計算により求める方法の概念図である。

#### 【0068】

図16は、コンテンツ配信サーバ101bから端末装置102に対して、コンテンツが時刻t2に送出開始される場合の例を示している。また、前述したように、コンテンツ配信サーバ101bではコンテンツの送出開始に先立ち、 $\beta$ だけ前（時刻t1）にECMを送出する必要がある。このとき、再生制御情報を生成するタイミング（時刻t0）は、再生制御情報やECMの生成に要する時間 $\alpha$ を考慮した上で決定する必要がある。ここで、 $\alpha$ は時間A～時間Dの和として表すことができ、具体的な時間A～時間Dの値として、時間Aがコンテンツ符号化部1105から時刻t0の時点でのPTSの値を取得するのに要する時間、時間Bがコンテンツの先頭のPTSの値を算出する時間、時間Cが再生制御情報を生成し、サブライセンス1000に設定するのに要する時間、時間DがECMを生成し、ワーク鍵Kw203、コンテンツ鍵Kc205で暗号化するのに要する時間、となる。すなわち、コンテンツの送出開始時のPTS1343aの値（コンテンツの先頭のPTS1343a）は、時刻t0にコンテンツ符号化部1105から取得したPTS1343aの値に、時間 $\alpha$ と時間 $\beta$ を加算した値として算出することができる。

#### 【0069】

なお、ここでは、制御範囲1514として、制御開始時刻と制御終了時刻に算出したPTS1343aの値をそのまま設定する場合の例を示したが、制御範囲1514にはPTS1343aの値を用いたコンテンツ先頭からの相対時刻を設定しておき、再生制御情報などにコンテンツ先頭のPTS1343aの値を別途設定するようにしても良い。このようすることにより、再生制御情報の生成処理（上述した時間Cに相当）における時刻情報の演算量を削減することができる。

#### 【0070】

このように生成した再生制御情報（制御情報1503）の例を、図17に示す。以下では、図15と図17とを用いて説明を行う。図17では、制御情報個数1510として「2」となっており、後述するように、プレビュー制御のための情報と、CMスキップ制御のための情報の2つの情報から構成されている。1つめの情報としては、制御ID1511として「プレビュー可」、制御期限1512が「2004/9/14」、制御回数1513が「1回」、制御範囲1514が「10000～100000」となっているので、当該コンテンツに関わるプレビュー制御としては、2004/9/14までの期間で、プレビューが可能な部分として、PTS1343aの値が10000～100000である部分を1回だけプレビューして良いことを示している。ここで、制御回数1513に関しては、端末装置102でのコンテンツ利用時に、コンテンツ再生箇所のPTS1343aを視聴履歴として記録し、該当箇所を何回視聴したかを管理することにより実現する。また、2つ目の情報として、制御ID1511が「特殊再生不可」、制御期限1512が「2004/7/6」、制御回数1513が「3回」、制御範囲1514が「20000～100000」、「500000～1000000」などなっているので、当該コンテンツのCM部分に関わる特殊再生制御としては、2004/9/14までの期間で、CMスキップが不可能な部分として、PTS1343aの値が20000～100000、500000～1000000などの部分を、少なくとも通常再生で3回視聴するように制御することを示している。

#### 【0071】

以上のように生成した再生制御情報を含む制御情報タグブロック1500は、サブライセンス1000に設定され、さらにECMに設定されるため、ECM生成部1107に送信される。なお、再生制御情報を設定するライセンスのIDを、再生制御情報中に設定するようにし、どのライセンスに対する再生制御情報かを明確に識別可能ないようにしても良い。

#### 【0072】

以下、再び図11に戻って、コンテンツ配信サーバ101bの構成についての説明を継続する。

ECM生成部1107は、スクランブル鍵Ks201やメインライセンス900を含むECMを生成する部である。具体的には、ECM生成部1107は、権利管理サーバ101aからワーク鍵Kw203、コンテンツ鍵Kc205、サブライセンス1000を受信するとともに、再生制御情報生成部1106から制御情報タグロック1500を受信する。上流システムからの指示によりECM-Kw、ECM-Kc、Kc配信用ECMを生成し、図11には図示しないスクランブル鍵生成部において生成したコンテンツのスクランブル鍵Ks201を設定するとともに、制御情報タグロック1500をサブライセンス1000に挿入して、Kc配信用ECMに設定する。さらに、生成した各ECMをワーク鍵Kw203、コンテンツ鍵Kc205により暗号化して、コンテンツ多重化部1108に生成したECMを送信する。また、生成したスクランブル鍵Ks201を、コンテンツを暗号化するコンテンツ暗号化部1109に送信する。

#### 【0073】

ここで、図18～図19を用いて、ECM-Kw、ECM-Kc、Kc配信用ECMのデータ構造についての詳細な説明を行う。

図18は、主としてスクランブル鍵Ks201を伝送するECMのデータ構造の一例を示す図である。端末装置102において、リアルタイム視聴用のワーク鍵Kw203で暗号化されたECM-Kw1800と、蓄積視聴用のコンテンツ鍵Ks205で暗号化されたECM-Kc1810のフォーマットは同一であり、暗号化を行う暗号鍵（ワーク鍵Kw203とコンテンツ鍵Ks205）が異なるのみである。

#### 【0074】

図18に示したECM-Kw1800、および、ECM-Kc1810は、スクランブル鍵Ks201やコンテンツに関する情報の伝送に用いられる情報であり、事業者ID1802、ワーク鍵ID1803、コンテンツID1804、スクランブル鍵Ks201、コンテンツ関連情報1806、改ざん検出1807とから構成されている。また、MPEG-2 Systemsのプライベートセクション形式でトランスポートストリームに多重化するため、セクションヘッダ1801、セクションテーラ（誤り検出）1807が付加されている。

#### 【0075】

事業者ID1802は、本コンテンツ利用制御システム1において、サービスを提供する事業者を識別するコードであって、次に述べるワーク鍵ID1803とともに参照される。

ワーク鍵ID1803は、ECMを暗号化するワーク鍵Kw203を識別するための情報であり、ECMの非暗号化部分に設定される。暗号化されたECMを復号する場合には、本ワーク鍵ID1803を参照することにより、どのワーク鍵Kw203を用いてECMを復号すれば良いかを判別することができる。

#### 【0076】

コンテンツID1804は、コンテンツ毎に割り当たられる識別子であり、本コンテンツ利用制御システム1において、コンテンツを一意に識別するためのコードである。

スクランブル鍵Ks201は、コンテンツのTSパケット1400のペイロード部（TSPayload1430）を暗号化する暗号鍵である。端末装置102が、数秒おきに変更されるスクランブル鍵Ks201を取得するのに要する時間を短縮するため、一般的にはスクランブル鍵201に複数の暗号鍵を設定する。

#### 【0077】

コンテンツ関連情報1806は、可変長のデータであり、コンテンツの属性などを示す情報が必要に応じて設定される。

改ざん検出1807は、暗号化されるECMの改ざんを検出するためのハッシュ値が設定される。

次に、図19は、主として蓄積視聴のためのECM-Kc1810を復号するためのコ

ンテンツ鍵Kc205を伝送するKc配信用ECMのデータ構造の一例を示す図である。

#### 【0078】

図19に示したKc配信用ECM1900は、コンテンツ鍵Kc205やサプライセンス1000の伝送に用いられる情報であり、事業者ID1902、ワーク鍵ID1903、サプライセンス1000、改ざん検出1904とから構成されている。コンテンツ鍵Kc205やコンテンツIDは、サプライセンス1000に含まれる。また、ECM-Kw1800およびECM-Kc1810と同様に、セクションヘッダ1901、セクションテーラ（誤り検出）1905が付加されている。

#### 【0079】

事業者ID1902、ワーク鍵ID1903、改ざん検出1904については、ECM-Kw1800およびECM-Kc1810における事業者ID1802、ワーク鍵ID1803、改ざん検出1808の説明と同様であるので、ここでは説明を省略する。また、サプライセンス1000については、図20に示すように、権利管理サーバ101aから取得したサプライセンス1000に、再生制御情報生成部1006から取得した制御情報タグブロック1500を挿入したデータ構造であり、図10および図15において、サプライセンス1000および制御情報タグブロック1500の各項目については説明済みであるので、ここでは説明を省略する。

#### 【0080】

なお、ECM-Kw1800、ECM-Kc1810、Kc配信用ECM1900に時刻情報を含めることもできる。各ECMは暗号化されて配信されるため、特にリアルタイム視聴においては、ECMに設定されたセキュアな時刻情報を用いた視聴制御などを行うことができる。

以下、再び図11に戻って、コンテンツ配信サーバ101bの構成についての説明を継続する。

#### 【0081】

コンテンツ多重化部1108は、コンテンツ符号化部1105から受け取った映像、音声、データなどを含むトランSPORTストリームと、ECM生成部1107から受け取った単数または複数のECMを含むトランSPORTストリームとを多重化し、多重化されたトランSPORTストリームをコンテンツ暗号化部1109に送出する部である。具体的には、コンテンツ多重化部1108は、コンテンツ符号化部1105から受信したTSパケット化されたコンテンツと、ECM生成部1107から受信したTSパケット化されたECM-Kw1800、ECM-Kc1810、Kc配信用ECM1900とを多重化して、端末装置102に送信するトランSPORTストリームを生成する。

#### 【0082】

コンテンツ暗号化部1109は、AESなどを用いてコンテンツを暗号化することにより、コンテンツの保護および時刻情報をコンテンツにセキュアにバインドする部である。具体的には、コンテンツ暗号化部909は、TSパケットのアダプテーションフィールドを除くペイロード部を、ECM生成部1107から取得したスクランブル鍵Ks201を用いて、CBC(Cipher Block Chaining)+OFB(Out put Feed Back)モードによって暗号化(スクランブル)する。これにより、時刻情報をコンテンツにセキュアにバインドしている。

#### 【0083】

コンテンツ送出部1110は、コンテンツ暗号化部1109において暗号化されたTSパケット1400を、端末装置102に送出する部である。具体的には、コンテンツ送出部1110は、コンテンツ暗号化部1109から受け取ったトランSPORTストリームを、放送波としてネットワーク103を通じて端末装置102に送出する。

なお、ここでは、コンテンツDB1101に蓄積されたコンテンツを読み出し、コンテンツ符号化部1105においてリアルタイムエンコードする場合の例を示したが、あらかじめオフラインでPES(ES)あるいはTSを生成しておき、コンテンツDB1101に蓄積しておくことにより、コンテンツ送出時にコンテンツ符号化部1105における工

ンコード処理を省略するようにしても良い。

#### 【0084】

また、ここでは、コンテンツDB1101に蓄積された非暗号のコンテンツを、コンテンツ暗号化部1109で送出時に暗号化する場合の例を示したが、あらかじめ暗号化されたMPEG-2 TSコンテンツを格納しておくようにすることもできる。

#### 【0085】

以上、図10～図20を用いて、配信センター101から端末装置102にコンテンツを送出するコンテンツ配信サーバ101bの構成についての詳細な説明を行った。また、図2～図20を用いて、配信センター101の各部分についての説明を行った。なお、配信センター101における課金サーバ101c、ウェブサーバ101dの詳細な構成については、本発明の主眼ではないため、ここでは省略する。

#### 【0086】

次に、コンテンツ利用制御システム1における端末装置102の構成について説明する。図21は、図1に示される端末装置102の詳細な構成を示す機能プロック図である。

端末装置102は、外部との通信インターフェースを提供する端末送受信部2101と、受信したトランスポートストリームをコンテンツとコンテンツ以外のデータとに分離する分離部2102と、コンテンツを蓄積するコンテンツ蓄積部2103と、ライセンスを処理、管理するライセンス処理部2104と、ライセンスを蓄積するライセンスDB2105と、セキュアにコンテンツの利用制御を行うコンテンツ利用制御部2106と、暗号化コンテンツの復号を行うコンテンツ復号部2107と、コンテンツを利用するコンテンツ利用部2108と、コンテンツの視聴箇所を視聴履歴として記録する視聴履歴記録部2109と、視聴履歴を蓄積する視聴履歴DB2110と、主としてユーザに対してインターフェースを提供する端末アプリケーション2111とから構成されている。

#### 【0087】

端末送受信部2101は、ネットワーク103を通じて、配信センター101と通信するための部である。

分離部2102は、MPEG-2 TSにより多重化された暗号化コンテンツを取得し、トランスポートストリームに含まれるPAT (Program Association Table)、PMT (Program Map Table)などのPSI情報を参照して、コンテンツの映像、音声、データや、ECM-Kw1800、ECM-Kc1810、Kc配信用ECM1900を含むTSパケット1400、および、PCR1425aが挿入されているTSパケット1400のPIDを取得し、コンテンツとECMを分離する部である。また、分離部2102は、同時に、PMTに記載されているPCR\_PID (PCRが含まれているPIDを示す)を参照することにより、TSパケット1400のAdaptation\_field1420にPCR1425aが挿入されているPIDのTSパケット1400を取得して、端末装置102でのコンテンツ再生の基準クロックとして、図21に図示しない計時部に供給する。また、コンテンツ蓄積部2103に一旦コンテンツを蓄積する場合には、PAT、PMTなどのPSI情報から必要な情報を選択してSIT (Selection Information Table)、DIT (Discontinuity Information Table)などのPSI情報の生成を行い、受信したトランスポートストリームを、パーシャルトランスポートストリーム（以下、パーシャルTSと記述する）と呼ばれるストリームを生成する処理を行う。

#### 【0088】

コンテンツ蓄積部2103は、生成したパーシャルTSを蓄積する部である。具体的には、コンテンツ蓄積部2103は、大容量HDDなどで実現され、分離部2102において受信したトランスポートストリームから生成したパーシャルTSを蓄積する。

ライセンス処理部2104は、ライセンスに基づき、セキュアにコンテンツの利用可否判定を行う。具体的には、ライセンス処理部2104は、ユーザからコンテンツの利用を要求された場合に、権利管理サーバ101aから取得したメインライセンス900、ある

いは、コンテンツとともに取得するサプライセンス1000に含まれる利用条件に基づき、コンテンツの利用が可能かどうかを判定する。そして、利用条件がコンテンツの利用を許諾している場合に限り、暗号化コンテンツを復号するための暗号鍵をコンテンツ利用制御部2106に渡す、という処理を行う。

#### 【0089】

例えば、ライセンス処理部2104は、メインライセンス900のライセンスヘッダ901に設定された有効期間914を参照し、コンテンツが利用可能であるかどうかを判定する。端末装置102に保持している、図21には図示しないセキュアな計時部により提供される現在時刻を参照し、現在時刻が有効期間914内である場合は、コンテンツの再生が可能であると判定するという処理を行う。

#### 【0090】

なお、ライセンス処理部2104とコンテンツ利用制御部2106とコンテンツ復号部2107との間は、コンテンツ鍵Kc205をセキュアに送受信するため、SACを確立して安全にコンテンツ鍵Kc205の送受信が行われる。但し、ライセンス処理部2104とコンテンツ利用制御部2106とコンテンツ復号部2107と、同じシステムLSI内などの同一耐タンパ領域にある場合は、安全にコンテンツ鍵Kc205の送受信を行うことができるので、必ずしもSACを確立する必要はない。

#### 【0091】

ライセンスDB2105は、セキュアにライセンスを管理するためのデータベースであり、ライセンス処理部2104により取得されたメインライセンス900などを蓄積する。具体的には、ライセンスDB2105は、図9で示される権利管理サーバ101aから取得したメインライセンス900などを蓄積、管理すると共に、改ざんなどの不正な行為を防止するため、ライセンスDB2105中のメインライセンス900などのハッシュ値を、ハード的またはソフト的に耐タンパ化された領域に格納する。

#### 【0092】

コンテンツ利用制御部2106は、ライセンス処理部2104からワーク鍵Kw203と利用条件とを用いて、セキュアにコンテンツの利用を制御するための部である。具体的には、コンテンツ利用制御部2106は、リアルタイム視聴時においては、分離部2102から受け取ったトランスポートストリームからECM-Kw1800のTSパケット1400を取得し、ECM-Kw1800を再構成する。このようにして得られたECM-Kw1800をワーク鍵Kw203により復号して、コンテンツをデスクランブルするためのスクランブル鍵Ks201を取得し、コンテンツ復号部2107に供給する。蓄積視聴時においては、コンテンツ蓄積部2103から読み出したトランスポートストリームから、Kc配信用ECM1900をワーク鍵Kw203により復号して、サプライセンス1000を取得する。そして、サプライセンス1000に含まれる利用条件判定を行った上で、コンテンツを利用可能である場合のみ、サプライセンス1000に含まれるコンテンツ鍵Kc205を用いて、ECM-Kc1810を復号して、スクランブル鍵Ks201を取得する。

#### 【0093】

さらに、コンテンツ利用制御部2106は、図21に図示しないセキュアな計時部を用いて、コンテンツの利用時間などを計時することにより、利用条件に従ったコンテンツ利用を制御する。

コンテンツ復号部2107は、暗号化されたコンテンツを復号する部である。具体的には、コンテンツ復号部2107は、暗号化されたMPEG-2 TSにより多重化されたコンテンツを取得し、トランスポートストリームに含まれるPAT、PMTなどのPSI情報を参照して、コンテンツの映像、音声、データを含むTSパケット、および、PCRが挿入されているTSパケットのPIDを取得する。そして、コンテンツ利用制御部2106から取得するスクランブル鍵Ks201によって、TSP Header1410中のtransport\_scrambling\_control（図14に図示せず）を参照して暗号化されているTSパケット1100のペイロードを復号する。

**【0094】**

コンテンツ利用部2108は、コンテンツをデコードして、図21に示さないモニターなどに出力するための部である。具体的には、コンテンツ利用部2108は、トランスポートストリーム中のPCR1425aを取得して、コンテンツ利用部2108が有するPLL(Phased Lock Loop)機能により、コンテンツ配信サーバ101bのSTC(計時部1103)と、コンテンツ利用部2108が有するSTC(図示せず)と同期させる。そして、TSパケット1400のTSP Pay load 1430からPESパケット1000のデータを取得して、MPGE-2あるいはMPEG-4の映像、音声、データなどのESをデコードして、モニターに出力する。また、コンテンツの利用を終了すると、利用終了通知をコンテンツ利用制御部2106に通知する。

**【0095】**

視聴履歴記録部2109は、コンテンツ利用部2108で視聴したコンテンツの視聴箇所の情報を視聴履歴として収集する。具体的には、視聴履歴記録部2109は、コンテンツ利用部2108で再生開始時および再生終了時のPTS1343aを取得し、このPTS1343aの値を視聴履歴として受け取り、UL(Usage Log、以下、ULと記述)として視聴履歴DB2110に蓄積する。ULのデータ構造については、後で図を用いて詳細に説明する。

**【0096】**

視聴履歴DB2110は、視聴履歴記録部2109により取得されたULを蓄積するデータベースである。ここで、ULのデータ構造について、図22を用いて説明する。

図22は、ULの構成の一例を示す図である。UL2200をコンテンツ利用制御システム1毎、あるいは、ユーザ毎で一意に特定可能な識別子であるUL識別子2201と、UL2200全体のサイズを示すULサイズ2202と、UL2200を生成したユーザを特定するためのユーザID2203と、UL2200を生成した端末装置102を特定するための端末ID2204と、ユーザが利用したコンテンツとUL2200とを関連づけるためのコンテンツID2205と、ユーザが利用したライセンス(メインライセンス900およびサブライセンス1000)とUL2200とを関連づけるためのライセンスID2206と、ユーザがコンテンツを操作した内容(種類)を特定するためのアクション種別2207と、ユーザがコンテンツの操作開始した絶対時刻である利用開始時刻2208と、UL2200に設定される時刻情報2210の個数を示す時刻情報個数2209と、コンテンツ利用部2208が取得するコンテンツの利用開始、利用終了時点での時刻情報(PESパケット1300のPTS1343a)の値である時刻情報2210とから構成されている。

**【0097】**

ここで、ライセンスID2206は、例えば、端末装置102から権利管理サーバ101aへメインライセンス900を返却するようなコンテンツ利用制御システムなどの場合、メインライセンス900とともにUL2200を収集することにより、ユーザが用いたメインライセンス900とサブライセンス1000の対応づけが可能となり、配信センター101において視聴履歴とライセンスとを関連づけて管理することができる。

**【0098】**

また、アクション種別2207は、「再生」、「コピー」、「印刷」などの、コンテンツに対するユーザのアクションを特定するための種別であって、サブライセンス1000のアクションID1021の値が設定される。ここでは、コンテンツの再生を示す「Play」の例が示されている。

さらに、時刻情報2210は、ユーザがコンテンツの利用を行った部分を特定するための情報であって、コンテンツの利用開始を表す時刻情報である開始時刻情報と、コンテンツの利用終了を表す時刻情報である終了時刻情報との組が、時刻情報個数2209に設定された個数分だけ存在する。ここでは、「開始時刻情報、終了時刻情報」の組がN個あり、「開始時刻情報1、終了時刻情報1」が「13970584、13999999」、「開始時刻情報N、終了時刻情報N」が「32141683、39705843970」で

ある場合が示されている。

なお、UL220.0には、UL220.0の改ざんを検出するためのハッシュ値などは存在していないが、必要に応じて改ざん検出を追加するようにしても良い。

#### 【0099】

以上、図22を用いて、端末装置102で記録する視聴履歴のデータ構造であるUL220.0について、その詳細な構成について説明を行った。なお、生成したUL220.0を必要に応じて任意のタイミング、もしくは、定期的に配信センター101に送信するようにしても良い。

#### 【0100】

端末アプリケーション211.1は、権利管理サーバ101aからメインライセンス900を取得したり、コンテンツの利用開始や終了を指示したりするインタフェースを提供する部である。具体的には、端末アプリケーション211.1は、ユーザの契約に応じたライセンスの取得要求として、期待ライセンス情報（Expected License Information、以下ELIと記述）を生成し、権利管理サーバ101aに送信することにより、権利管理サーバ101aからライセンスを取得する。

#### 【0101】

図23はELIの一例を示す図である。ELI2300は、ELI識別子2301と、端末ID2302と、利用条件ID2303と、契約ID2304とから構成される。ELI識別子2301には、このデータがELI2300であることを示す情報が記述される。端末ID2302には、ELI2300を生成した端末装置102、すなわち、ライセンスを要求する端末装置102の端末IDが記述される。利用条件ID2303には、権利管理サーバ101aの利用条件DB203において管理されるユーザの利用条件を特定するための利用条件ID702が記述される。この利用条件ID702は、ユーザが権利管理サーバ101aから利用可能な権利を問い合わせる際のレスポンスで通知される利用条件IDを使用する。契約ID2304は、メインライセンス900に対応する契約IDを記述する。なお、上記に加えて、ユーザが期待するライセンスの有効期間（メインライセンス900のライセンスヘッダ901に記載される有効期間915、またはサプライセンス1000のライセンスヘッダ1001に記載される有効期間1015）を要求するようにしても良い。

#### 【0102】

なお、端末装置102のうち、特にセキュリティを必要とするデータを処理する部、具体的には、ライセンス処理部2104、ライセンスDB2105、コンテンツ利用制御部2106、コンテンツ復号部2107、コンテンツ利用部2108、視聴履歴記録部2109、視聴履歴DB2110は、悪意のあるユーザなどによる不正な利用を防止するため、ハードウェア的に耐タンパ化されたシステムLSIや、ソフトウェア的に耐タンパ化されたプログラムなどで実現されるのが一般的である。また、端末装置102をコンテンツ利用制御システム1内で一意に特定するためのID（端末ID）についても、図21に図示しない耐タンパ化された場所に保持しているものとする。

以上、図21～図23を用いて、端末装置102についての詳細な構成の説明を行った。

#### 【0103】

さて、以上のように構成された端末装置102において、ユーザが配信センター101からコンテンツおよびライセンスを取得し、セキュアにコンテンツを利用するとともに、再生制御情報やコンテンツの視聴履歴を用いてコンテンツの視聴をセキュアに制御するという一連の動作を、図24～図32に示すフローチャートを用いて説明する。

#### 【0104】

なお、ユーザが権利管理サーバ101aからメインライセンス900を取得するにあたって、事前にウェブサーバ101dなどを用いたサービスプロバイダへの会員登録、コンテンツの利用条件の購入などの処理が必要であるが、これらの処理については本発明の主眼ではないため、以下の説明では省略する。

最初に、端末装置102において、ユーザが権利管理サーバ101aからメインライセンス900を取得する動作を、図24に示すフローチャートを用いて説明する。

#### 【0105】

まずユーザが、端末アプリケーション2111が提供するユーザインターフェースにより、権利管理サーバ101aで管理されているユーザの利用条件（ライセンス）一覧を取得し、利用条件一覧から取得したい契約に対するライセンスを選択すると、端末装置102は、メインライセンス900を権利管理サーバ101aに要求するためのELI2300を作成し、権利管理サーバ101aに送信する（ステップS2401）。

#### 【0106】

具体的には、端末アプリケーション2111は、ユーザの契約に対応する契約IDをライセンス処理部2104に送信する。ライセンス処理部2104は、受け取った契約IDを基に図23に示したELI2300を生成する。なお、このELI2300に設定する利用条件ID2303は、端末アプリケーション2111またはライセンス処理部2104が、あらかじめユーザが所有する利用条件を権利管理サーバ101aに直接問い合わせるか、または、ウェブサーバ101d経由で問い合わせることにより、利用条件ID2303を取得済みであるものとする。このようにして生成したELI2300を、端末送受信部2101を通じて、権利管理サーバ101aに送信する。なお、メインライセンス900は、その有効期限の間は権利管理サーバ101aから1回だけ取得すれば良い。

#### 【0107】

権利管理サーバ101aのライセンス発行部311は、サーバ送受信部312が端末装置102から受信したELI2300を受け取ると、ユーザ情報DB302を参照し、ユーザを特定することにより、ユーザ認証を行う（ステップS2402）。

具体的には、ユーザ認証は2段階で行なわれる。通常、ライセンスのようなセキュリティを要するデータのやり取りを行う際には、SACを確立して安全に通信を行えるようるのが一般的である。よって、第1段階としては、権利管理サーバ101aと端末装置102との間でSSLやTLSによりSACを確立する。この相互認証によって、権利管理サーバ101aは、端末装置102が正しい端末ID2302を有することが確認できる。第2段階として、ライセンス発行部311が端末ID2302なる端末装置102を所有するユーザを特定する。そこでライセンス発行部311は、ELI2300に含まれる端末ID2302を取得し、ユーザ情報DB302のユーザ情報管理テーブル600のユーザID601および端末ID602を参照して、ELI2300に含まれる端末ID2302と一致するユーザ情報管理テーブル600の端末ID602を検索する。一致する端末ID602が見つかった場合には、関連するユーザID601を取得することができるが、一致する端末ID602が見つからなかった場合には、ユーザ認証は失敗する。

#### 【0108】

ライセンス発行部311は、ステップS2402のユーザ認証結果を確認する（ステップS2403）。

ステップS2403において、YESである場合、すなわち、正しくユーザ認証が行なわれた場合には、メインライセンス900を発行するための利用条件の確認を行うため、ステップS2404を実行する。

#### 【0109】

ステップS2403において、NOである場合、すなわち、正しくユーザ認証が行なわれなかつた場合には、ライセンス発行不可と判定され、ライセンス発行部311はライセンス発行不可通知を端末装置102に送信する。

ライセンス発行部311は、ライセンス発行可否判定処理を実行する（ステップS2404）。このライセンス発行可否判定処理については、後で図24を用いて詳細に説明する。

#### 【0110】

ライセンス発行部311は、ライセンス発行可否判定処理の結果を参照し、メインライセンス900が発行可能か否かを判定する（ステップS2405）。

ステップS2405において、YESである場合、すなわち、ライセンス発行可能と判定された場合には、ステップS2406を実行する。

ステップS2405において、NOである場合、すなわち、ライセンス発行不可と判定された場合には、ライセンス発行部311はライセンス発行不可通知を端末装置102に送信する。

#### 【0111】

ライセンス発行部311は、メインライセンス900を生成する（ステップS2406）。具体的には、ライセンス発行部311は、ELI2300および利用条件DB303の利用条件管理テーブル700を参照するとともに、鍵情報DB301のワーク鍵管理テーブル400から、契約ID2204（契約ID401）に対応するワーク鍵Kw203を取得し、ELI2300により要求されたメインライセンス900を生成する。

#### 【0112】

ライセンス発行部311は、利用条件DB303の利用条件管理テーブル700を更新する（ステップS2407）。具体的には、ライセンス発行部311は、発行したメインライセンス900に含まれる利用条件の分だけ、当該ユーザの利用条件を減算する処理を行う。例えば、利用条件管理テーブル700において、ユーザID701が「USER-ID-00003」、利用条件ID702が「URUs-ID-24024」の利用条件に対するメインライセンス900の発行を要求された場合、発行可能残回数705が「2」であるので、利用条件管理テーブル700の発行可能残回数705を「1」に更新するという処理を行う。

#### 【0113】

ライセンス発行部311は、ステップS2406において生成したメインライセンス900を端末装置102に送信する（ステップS2408）。具体的には、ライセンス発行部311は、サーバ送受信部312を通じて、端末装置102にメインライセンス900を送信する処理を行う。

端末装置102のライセンス処理部2104は、権利管理サーバ101aから受信したメインライセンス900を受け取り、メインライセンス900をライセンスDB2105に登録する（ステップS2409）。具体的には、ライセンス処理部2104は、端末送受信部2101を通じて、ステップS2401で生成したELI2300に対するレスポンスとしてメインライセンス900を取得し、メインライセンス900をライセンスDB2105に書き込み、ライセンスDB2105のハッシュ値を更新する。

#### 【0114】

なお、ステップS2403またはステップS2405において、メインライセンス900が発行不可であるためにライセンス発行不可通知が送信された場合、端末装置102のライセンス処理部2104は、ライセンス発行不可通知を受信する（ステップS2410）。具体的には、端末装置102のライセンス処理部2104は、権利管理サーバ101aからのライセンス発行不可通知を受信し、端末アプリケーション2111のユーザインターフェースを通じて、ユーザにその旨を通知して、本処理を終了する。

#### 【0115】

ここで、ステップS2404のライセンス発行可否判定処理について、図25を用いて説明する。

まず、ライセンス発行部311は、ELI2300で指定された利用条件ID2203が利用条件DB303の利用条件管理テーブル700に存在するかどうかを確認する（ステップS2501）。具体的には、ライセンス発行部311は、端末装置102から受信したELI2300を参照し、利用条件ID2203を取得する。この利用条件ID2203が、利用条件管理テーブル700中の利用条件ID702と一致するものがあるかどうかを確認する。

#### 【0116】

ステップS2501において、YESである場合、すなわち、利用条件管理テーブル700にELI2300の利用条件ID2203と一致する利用条件ID702が存在する

場合には、さらに、利用条件ID702を有するユーザID701が、図24におけるステップS2402で認証に成功した、ユーザ情報DB302のユーザ情報管理テーブル600中のユーザID601と一致するかどうかを確認する。ここで当該ユーザIDが一致した場合には、ステップS2502を実行し、当該ユーザIDが一致しない場合には、ステップS2505を実行する。

#### 【0117】

ステップS2501において、NOである場合、すなわち、利用条件管理テーブル700にELI2300の利用条件ID2203と一致する利用条件ID702が存在しない場合には、ステップS2505を実行する。

次に、ライセンス発行部311は、ユーザの利用条件が、有効期限を満たしているかどうかを判定する（ステップS2502）。具体的には、ライセンス発行部311は、利用条件DB303の利用条件管理テーブル700中の有効期間704を参照するとともに、セキュアな計時部（図2に図示せず）から現在時刻を取得し、現在時刻が有効期間704で示される開始日時から終了日時の間に含まれているか否かを判定する。

#### 【0118】

例えば、利用条件管理テーブル700中の有効期間704が「2002/12/20 12:12:12」である場合に、現在時刻が「2002/12/18 12:34:56」であれば、ユーザの利用条件が有効期限内であると判定し、現在時刻が「2002/12/31 19:00:00」であれば、ユーザの利用条件は有効期限外であると判定する。

#### 【0119】

ステップS2502において、YESである場合、すなわち、ユーザの利用条件が有効期限内である場合には、ステップS2503を実行する。

ステップS2502において、NOである場合、すなわち、ユーザの利用条件が有効期限外である場合には、ステップS2505を実行する。

ライセンス発行部311は、ライセンスの発行可能回数が残っているかどうかを判定する（ステップS2503）。具体的には、ライセンス発行部311は、利用条件管理テーブル700の発行可能残回数705が1以上であるかどうかを確認する。例えば、利用条件管理テーブル700の発行可能残回数が「2」である場合には、ライセンスが発行可能であると判定し、「0」である場合には、ライセンスが発行不可であると判定する。

#### 【0120】

ステップS2503において、YESである場合、発行可能残回数705が1以上である場合には、ステップS2504を実行する。

ステップS2503において、NOである場合、すなわち、発行可能残回数705が0である場合には、ステップS2505を実行する。

ライセンス発行部311は、メインライセンス900が発行可能と判定して、ライセンス発行可否判定処理を終了する（ステップS2504）。

#### 【0121】

また、ステップS2501～ステップS2503において、NOである場合、すなわち、ライセンス発行部311がメインライセンス900を発行不可能と判定した場合には、ライセンス発行可否判定処理を終了する（ステップS2505）。

以上、図25を用いて、ライセンス発行可否判定処理の説明を行った。

次に、権利管理サーバ101aにおける、サブライセンス1000の生成処理、および、ワーク鍵Kw203、コンテンツ鍵Kc205、サブライセンス1000のコンテンツ配信サーバ101bへの送信処理について、図26を用いて説明する。

#### 【0122】

権利管理サーバ101aは、コンテンツ配信サーバ101bからのワーク鍵Kw203、コンテンツ鍵Kc205、および、サブライセンス1000の要求を、LAN101nを通じて図3に図示しない要求受信部で受信すると、ライセンス発行部311は、データベース部300のコンテンツ情報DB304から、対応するコンテンツに関する情報を取

得する（ステップS2601）。具体的には、ライセンス発行部311は、コンテンツ配信サーバ101bからの要求に含まれるコンテンツIDに基づき、コンテンツ情報DB304のコンテンツ情報管理テーブル800から、サプライセンス1000を生成するために必要な利用条件として、ライセンスID802、有効期間803、利用可能回数804を取得する。

#### 【0123】

ライセンス発行部311は、データベース部300の鍵情報DB301から、契約に対応するワーク鍵Kw203およびコンテンツにコンテンツ鍵Kc205を取得する（ステップS2602）、具体的には、ライセンス発行部311は、コンテンツ配信サーバ101bからの要求に含まれる契約IDおよびコンテンツIDに基づき、鍵情報DB301のワーク鍵管理テーブル400およびコンテンツ鍵管理テーブル500から、契約ID401およびコンテンツID501に一致するワーク鍵Kw203およびコンテンツ鍵Kc205を取得する。なお、ワーク鍵管理テーブル400およびコンテンツ鍵管理テーブル500中に、コンテンツ配信サーバ101bからの要求に対応する契約ID401およびコンテンツID501が存在しない場合については、図26には示していないが、この場合は、エラーとしてコンテンツ配信サーバ101bにその旨を通知する処理を行う。

#### 【0124】

ライセンス発行部311は、サプライセンス1000を生成する（ステップS2603）。具体的には、ライセンス発行部311は、コンテンツ情報DB304のコンテンツ情報管理テーブル800から取得した該当コンテンツの利用条件と、鍵情報DB301のコンテンツ鍵管理テーブル500から取得した該当コンテンツのコンテンツ鍵Kc205とを用いて、図10に示したサプライセンスを生成する。

#### 【0125】

ライセンス発行部311は、生成したサプライセンス1000と、ワーク鍵Kw203、コンテンツ鍵Kc205をコンテンツ配信サーバ101bに送信する（ステップS2604）。具体的には、ライセンス発行部311は、ステップS2603において生成したサプライセンス1000と、鍵情報DB301のワーク鍵管理テーブル400から取得したワーク鍵Kw203と、鍵情報DB301のコンテンツ鍵管理テーブル500から取得したコンテンツ鍵Kc205とを、LAN101nを通じてコンテンツ配信サーバ101bに送信する。

#### 【0126】

次に、コンテンツ配信サーバ101bのECM生成処理、および、コンテンツ送信処理について、図27を用いて説明する。

コンテンツ配信サーバ101bにおいて、再生制御情報生成部1106は、コンテンツ送出指示により、コンテンツ符号化部1105から現在のPTS1343aを取得し、コンテンツの先頭のPTS1343aの値を算出する（ステップS2701）。具体的には、再生制御情報生成部1106は、番組運行管理システムなどの図11に図示しない上流システムからのコンテンツ送出指示を受けると、コンテンツ符号化部1105から、この時点でのPTS1343aの値、すなわち、時刻情報付加部1104により設定されたSTCの値を取得する。このように取得したPTS1343aの値（図16における時刻t0）を用いて、図16において説明した方法により、コンテンツの先頭でのPTS1343aの値（図16における時刻t2）を算出し、これを内部で保持する。

#### 【0127】

再生制御情報生成部1106は、コンテンツ属性情報DB1102の情報に基づいて再生制御情報を生成して、ECM生成部1107に送信する（ステップS2702）。具体的には、再生制御情報生成部1106は、コンテンツ属性DB1102のコンテンツ属性情報管理テーブル1200を参照し、該当するコンテンツID1201のプレビュー可能区間1203およびCM区間1104を取得して、必要に応じてプレビュー制御のための再生制御情報やCMスキップ制御のための再生制御情報を生成する。このとき、ステップS2701で算出したコンテンツの先頭でのPTS1343aの値を用いて、コンテンツ

属性情報管理テーブル1200での時刻情報の記述を、PTS1343aを用いた記述に変換する。

#### 【0128】

コンテンツ送出部1010は、コンテンツの送出が完了したか否かを判定する（ステップS2703）。具体的には、コンテンツ送出部1110は、コンテンツの全てをTSパケット1400として端末装置102に送出したか否かを判定する。

ステップS2703において、NOである場合、すなわち、コンテンツの送出が完了していない場合には、ステップS2704を実行する。

#### 【0129】

ステップS2703において、YESである場合、すなわち、コンテンツの送出が全て完了した場合には、その旨をコンテンツ符号化部1105や再生制御情報生成部1106、あるいは、上流システムなどに通知して、本処理を終了する。

ECM生成部1107は、再生制御情報生成部1106から受信する再生制御情報と、権利管理サーバ101aから受信するサプライセンス1000、ワーク鍵Kw203、コンテンツ鍵Kc205とを用いて、ECMを生成、暗号化して、生成したECMをコンテンツ多重化部1108に送信する（ステップS2704）。具体的には、ECM生成部1107は、図18に示した事業者ID1801やコンテンツ関連情報1806など、ECMを生成するために必要な情報をデータベース（図11に示さず）などから取得し、平文のECM-Kw1800、ECM-Kc1810を生成して、権利管理サーバ101aから受信した、対応するワーク鍵Kw203、コンテンツ鍵Kc205で暗号化して、暗号化されたECM-Kw1800、ECM-Kc1810を生成する。また、再生制御情報生成部1106から取得した再生制御情報（制御情報タグブロック1503）を、権利管理サーバ101aから受信したサプライセンス1000に設定して、事業者ID1901などを用いて平文のKc配信用ECM1900を生成する。平文のKc配信用ECM1900に対して、ワーク鍵Kw203を用いて暗号化することにより、暗号化されたKc配信用ECM1900が生成される。このように生成されたECM-Kw1800、ECM-Kc1810、および、Kc配信用ECM1900は、TSパケット化された後、コンテンツ多重化部1108に送信される。

#### 【0130】

また、ECM生成部1107は、内部で生成し、数秒おきに更新されるスクランブル鍵Ks201を、暗号化すべきTSパケット1400のPIDとともに、順次コンテンツ暗号化部1109に送信する処理を行う。

コンテンツ符号化部1105は、コンテンツDB1101から、該当コンテンツIDのコンテンツを読み出す（ステップS2705）。具体的には、コンテンツ符号化部1105は、上流システム（図11に図示せず）から受け取ったコンテンツIDをキーとしてコンテンツDB1101を検索し、該当コンテンツを順次読み出す処理を行う。

#### 【0131】

コンテンツ符号化部1105は、コンテンツDB1101から読み出したコンテンツをエンコードして、PESパケット1300、TSパケット1400を順次生成するとともに、時刻情報を付加する（ステップS2706）。具体的には、コンテンツ符号化部1105は、ステップS2705においてコンテンツDB1101から読み出したコンテンツの映像、音声などを順次MPEGエンコードし、時刻情報付与部1104から取得したSTCを用いて、映像ES、音声ESの同期を実現するためのPTS1343a、DTS1343bを付与する。さらに、PESパケット1300をTSパケット化するとともに、時刻情報付与部1104から取得したSTCを用いて、端末装置102内の基準クロックを、コンテンツ配信サーバ101bの基準クロック（計時部1003）と同期させるためのPCR1425aを付与する。

#### 【0132】

コンテンツ多重化部1108は、コンテンツとECMなどを多重化して、コンテンツ暗号化部1109に送信する（ステップS2707）。具体的には、コンテンツ多重化部1

108は、コンテンツ符号化部1105から取得したコンテンツのTSパケット1400と、ECM生成部1107から取得したECM-Kw1800、ECM-Kc1810、Kc配信用ECM1900のTSパケット1400とを多重化することにより、コンテンツと関連する情報が多重化されたトランSPORTストリームを生成する。このとき、コンテンツ多重化部1108は、PSI(PAT、PMTなど)、スルパケットなどの他のTSパケット1400も生成し、コンテンツやECMのTSパケット1400と共に多重する。また、必要に応じてPCR1425aの補正を行う。このように生成したトランSPORTストリームを、コンテンツ暗号化部1109に送信する。

#### 【0133】

コンテンツ暗号化部1109においてトランSPORTストリームをスクランブルした後、コンテンツ送出部1110からトランSPORTストリームを送信する(ステップS2708)。具体的には、コンテンツ暗号化部1109は、コンテンツ多重化部1108から受信したトランSPORTストリームに対し、ECM生成部1107から取得したスクランブルすべき映像、音声などのPIDを用いて、TSパケット1400のペイロード部(TSPayload1430)をECM生成部1107から順次取得するスクランブル鍵Ks201でスクランブルする。

#### 【0134】

また、コンテンツ送出部1110は、コンテンツ暗号化部1109から受け取った暗号化されたTSパケット1400を、順次端末装置102に伝送する。その後、ステップS2703を実行する。

以上、コンテンツ配信サーバ101bにおけるコンテンツの送出を行う動作についての説明を終了する。

#### 【0135】

次に、端末装置102において、ユーザがコンテンツ蓄積部2103に蓄積されたコンテンツを蓄積視聴する動作を、図28に示すフローチャートを用いて説明する。

まずユーザは、端末アプリケーション2111を通じて、コンテンツ一覧から利用したいコンテンツを選択する。コンテンツ利用制御部2106に通知された該当コンテンツに対応するライセンスIDが、ライセンス処理部2104に送信される(ステップS2801)。具体的には、コンテンツ利用制御部2106は、ユーザが選択したコンテンツIDおよびコンテンツの位置を示すURI(Unified Resource Identifier)を端末アプリケーション2111から受け取り、端末装置102が保持するコンテンツに関するメタデータなどを用いて、コンテンツIDに対するライセンスIDを取得する。このとき、当該コンテンツIDがサブスクリプションコンテンツであり、何らかの契約IDと関連付けられている場合には、当該契約IDに対応するライセンスIDを取得する。このように取得したライセンスIDをライセンス処理部2104に送信することにより、該当コンテンツの利用を要求する。

#### 【0136】

ライセンス処理部2104は、ライセンスDB2105から、該当ライセンスIDに対応するライセンスを取得する(ステップS2802)。具体的には、ライセンス処理部2104は、コンテンツ利用制御部2106から受信したライセンスIDをキーとしてライセンスDB2105を検索する。

ライセンス処理部2104は、ステップS2802において検索したライセンスを取得し、利用可能なライセンスであるか否かを判定する(ステップS2803)。具体的には、ライセンス処理部2104は、まず、コンテンツ利用制御部2106から指定されたライセンスIDを有するライセンスが、ライセンスDB2105に存在するかどうかを確認する。該当ライセンスが存在する場合には、ライセンスの有効期間などを参照し、ライセンスの有効性を確認する。なお、有効期間の有効性の確認については、端末装置102内のセキュアな計時部(図21に図示せず)から取得した時刻情報を用いて確認するものとする。なお、コンテンツ利用制御部2106から指定されたライセンスIDに対応するライセンスがライセンスDB2106に存在しない場合は、ステップS2807を実行する。

## 【0137】

ステップS2803において、YESである場合、すなわち、ライセンスが利用可能であると判定された場合には、ステップS2804を実行する。

ステップS2803において、NOである場合、すなわち、ライセンスが利用不可能であると判定された場合には、ステップS2807を実行する。

ライセンス処理部2104は、メインライセンス900を取得し、ワーク鍵Kw203を取得する（ステップS2804）。具体的には、ライセンス処理部2104は、メインライセンス900の暗号鍵タグブロック903に設定されたワーク鍵Kw203を取得し、内部で保持する。

## 【0138】

ライセンス処理部2104は、Kc配信用ECM1900に含まれるサプライセンス1000を取得することにより、コンテンツ鍵Kc205および再生制御情報を取得して、コンテンツ利用制御部2106に送信する（ステップS2805）。具体的には、ライセンス処理部2104は、分離部2102で分離されたKc配信用ECM1900を取得すると、メインライセンス900から得られたワーク鍵Kw203により、暗号化されたKc配信用ECM1900を復号する。Kc配信用ECM1900に含まれるサプライセンス1000を取得すると、ステップS2803で示したメインライセンス900の有効性判定と同様な方法によりサプライセンス1000の有効性を確認した上で、サプライセンス1000の暗号鍵タグブロック1003に含まれるコンテンツ鍵Kc205を取得する。また、制御情報タグブロック1500に含まれる再生制御情報（制御情報1503）を取得する。このように取得したコンテンツ鍵Kc205および再生制御情報を、必要に応じてSACを確立し、コンテンツ利用制御部2106に送信する。なお、コンテンツ鍵Kc205は、コンテンツのスクランブル鍵Ks201を取得するため、コンテンツ復号部2107に送信される。

## 【0139】

コンテンツ復号部2107およびコンテンツ利用部2108は、コンテンツ利用制御部2106が取得したコンテンツ鍵Kc205および再生制御情報に基づき、セキュアにコンテンツの利用を行う（ステップ2806）。

なお、ステップS2803において、利用可能なライセンスが存在しない場合には、コンテンツ利用制御部2106は、ライセンス処理部2104から利用不可通知を受信する（ステップS2807）。コンテンツ利用制御部2106は、端末アプリケーション2111が提供するユーザインタフェース部を通じて、ユーザにその旨を通知する。

## 【0140】

ここで、ステップS2806のコンテンツ利用処理について、図29を用いて説明する。

コンテンツ利用制御部2106は、コンテンツの受信を端末送受信部2101に指示し、コンテンツ配信サーバ101bから当該コンテンツを受信する（ステップS2901）。具体的には、コンテンツ利用制御部2106は、端末アプリケーション2111から受信したコンテンツのURI（デジタル放送の場合はチャネルに相当）を基に、コンテンツ配信サーバ101bから送信されたコンテンツを受信する。

## 【0141】

コンテンツ利用制御部2106は、コンテンツの再生が完了したかどうかを判定する（ステップS2902）。具体的には、コンテンツ利用制御部2106は、端末アプリケーション2111からコンテンツ再生終了指示が送信された場合や、コンテンツ配信サーバ101bからのコンテンツ受信が完了したか否か、もしくは、コンテンツの切れ目（変わり目）をPSI/SIなどを用いて検出したりすることにより、コンテンツの再生が完了したかどうかを判定する。

## 【0142】

ステップS2902において、NOである場合、すなわち、コンテンツの再生が完了し

ていない場合には、ステップS2904を実行する。

ステップS2902において、YESである場合、すなわち、ユーザから端末アプリケーション2111を通じて、コンテンツ再生終了の通知を受けた場合や、コンテンツの受信が完了した場合には、端末アプリケーション2111を通じてその旨をユーザに通知し、本処理を終了する。

#### 【0143】

コンテンツ復号部2107は、ECM-Kc1810のTSパケット1400を取得して、スクランブル鍵Ks201を取得する（ステップS2903）。具体的には、コンテンツ復号部2107は、分離部2902から受信したECM-Kc1810のTSパケット1400からECM-Kc1810を再構成して、コンテンツ利用制御部2106から取得したコンテンツ鍵Kc205を用いて、暗号化されたECM-Kc1810を復号し、スクランブル鍵Ks201を取得して内部レジスタなどに保持する。

#### 【0144】

コンテンツ復号部2107は、コンテンツのTSパケット1400を取得して、内部レジスタに保持したスクランブル鍵Ks201を用いてTSパケット1400のデスクランブルを行い、再構成したコンテンツのデコードを実行する（ステップS2904）。具体的には、コンテンツ復号部2107は、TSP Header1410中のtransport\_scrambling\_controlを参照することによって、ペイロード部（TSP Payload1430）が暗号化されているTSパケット1400を、スクランブル鍵Ks201を用いてデスクランブルし、デスクランブルされたTSパケット1400を順次コンテンツ利用部2108に送信する。コンテンツ利用部2108は、コンテンツ復号部2107から復号されたTSパケット1400を受信し、TSパケット1400のペイロード部（TSP Payload1430）から復号されたPESパケット1400を取得し、コンテンツの映像ES、音声ESなどのデータを取得して、それぞれのESをデコードして、映像、音声の同期をとりつつ、図21に示さないモニターなどに出力する。このとき、コンテンツ利用部2108は、TSパケット1400のAdaptation Field1420のPCR1425aを取得し、コンテンツ利用部2108の内部に有するSTCを、PLL（図15に図示せず）を用いることにより、安定したクロックに保つ処理を行う。よって、このSTCの値と、PESパケット1300のPTS1343a、DTS1343bが一致したときにPESパケット1300のPES Packet Data Bytes1360の映像ES、音声ESなどのデコード、表示を行うことにより、正常なコンテンツ再生を実現する。

#### 【0145】

視聴履歴記録部2109は、コンテンツ利用部2108で表示したコンテンツのPTS1343aを取得して、視聴履歴DB2110に記録する（ステップS2905）。具体的には、視聴履歴記録部2109は、コンテンツ利用部2108がコンテンツを再生した時点のPTS1343aの値（表示したPESパケット1300に含まれるPTS1343a）をコンテンツ利用部2108から取得し、少なくともコンテンツの再生開始および再生終了時点でのPTS1343aの値を視聴履歴として視聴履歴DB2110に記録する。なお、PTS1343aの記録は、視聴履歴DB2110のデータベース処理負荷を低減するため、表示したPTS1343aの値を隨時内部メモリに保持、更新しておき、適当なタイミングで視聴履歴DB2110をアップデートするようにしても良い。また、セキュアな計時部（図21に図示せず）から取得した日時情報、ユーザが指示したアクションである「Play（再生）」、再生を行ったユーザIDや端末IDとともに記録することにより、図22で示したUL2200が生成され、視聴履歴DB2110に蓄積される。

#### 【0146】

なお、リアルタイム視聴時における端末装置102の動作については、図28で説明したステップS2805において、コンテンツ鍵Kc205の代わりにワーク鍵Kw203を取得し、ワーク鍵Kw203を用いてECM-Kw1800を復号することによりスク

ランブル鍵Ks201が得られる点が図28に示すフローチャートと異なるだけであり、他のステップについては図28および図29と同様であるので、ここでは説明を省略する。

#### 【0147】

次に、図28および図29で示した蓄積コンテンツの視聴中において、コンテンツのタイムスキップを行う場合の動作を、図30に示すフローチャートを用いて説明する。

ユーザが、端末アプリケーション2111を通じて、再生中のコンテンツのタイムスキップを要求すると、コンテンツ利用制御部2106は、スキップ先の位置を取得する（ステップS3001）。具体的には、コンテンツ利用制御部2106は、ユーザにより指定されたスキップ先についての時刻情報（現在再生している箇所からの秒数など）を取得する。

#### 【0148】

コンテンツ利用制御部2106は、現在の再生箇所のPTS1343a（以下、PTS\_srcと記述）と、スキップ先のPTS1343a（以下、PTS\_dstと記述）を取得する（ステップS3002）。具体的には、コンテンツ利用制御部2106は、コンテンツ利用部2108から現在再生している箇所のPTS1343a（最近に表示したフレームに付与されていたPTS1343a）を取得するとともに、ステップS3001で取得したスキップ先の時刻情報を、PTS1343aに基づく値に変換する。例えば、ステップS3001で取得した時刻情報が現在再生している箇所からの秒数である場合には、PTS\_srcに当該時刻情報をPTS1343aのクロックである90000で除した値を加算することにより、スキップ先のPTS1343aであるPTS\_dstの値が得られる。なお、コンテンツ利用制御部2106がPTS\_srcの値を取得する方法の一例としては、外部からアクセス可能なコンテンツ利用部2108の内部レジスタに、現在再生している箇所のPTS1343aの値を隨時書き込む方法が挙げられる。

#### 【0149】

コンテンツ利用制御部2106は、ライセンス処理部2104から取得した再生制御情報に基づき、タイムスキップ（特殊再生）の制御期間内であるかどうかを判定する（ステップS3003）。具体的には、コンテンツ利用制御部2106は、再生制御情報（制御情報1503）の制御ID1511が「特殊再生不可」となっている情報を含む場合に、セキュアな計時部（図21に図示せず）から取得した日時情報と制御期限1512の値とを比較することにより、現在が特殊再生を制御すべき期間であるかどうかを判定する。

#### 【0150】

ステップS3003において、YESである場合、すなわち、現在が特殊再生を制御すべき期間である場合には、ステップS3004を実行する。

ステップS3003において、NOである場合、すなわち、現在が特殊再生を制御すべき期間でない場合には、ステップS3006を実行する。

コンテンツ利用制御部2106は、ライセンス処理部2104から取得した再生制御情報に基づき、タイムスキップ（特殊再生）を行える区間であるかどうかを判定する（ステップS3004）。具体的には、コンテンツ利用制御部2106は、再生制御情報（制御情報1503）の制御ID1511が「特殊再生不可」となっている情報を含む場合に、制御範囲1514で指定されるPTS1343aの範囲である制御開始時刻～制御終了時刻が、PTS\_src～PTS\_dstに含まれるかどうかを、制御時刻個数1520の分だけチェックする。すなわち、現在再生している箇所とスキップ先の箇所とで表される区間が、少なくとも1つのCMスキップ禁止区間の一部または全部（制御情報1503の制御開始時刻～制御終了時刻）を包含する場合を検出している。

#### 【0151】

ステップS3004において、YESである場合、すなわち、PTS\_src～PTS\_dstにCMスキップ禁止箇所が含まれる場合は、ステップS3005を実行する。

ステップS3004において、NOである場合、すなわち、PTS\_src～PTS\_dstにCMスキップ禁止箇所が含まれない場合は、ステップS3006を実行する。

コンテンツ利用制御部2106は、当該コンテンツの視聴履歴を取得して、PTS\_Src～PTS\_Dstに含まれるCMスキップ禁止箇所の過去の視聴回数が、規定数以上であるかどうかを判定する（ステップS3005）。具体的には、コンテンツ利用制御部2106は、視聴履歴DB2106を検索して、視聴履歴DB2106に蓄積されたUL2200の内、コンテンツID2205が一致するUL2200の視聴履歴である時刻情報2210を参照する。時刻情報2210は、当該コンテンツを過去に視聴したPTS1343aの値が記載されているので、PTS\_Src～PTS\_Dstに含まれるCMスキップ禁止箇所が含まれている回数をカウントして、制御情報1503の制御回数1513と比較する処理を行う。

#### 【0152】

ステップS3005において、PTS\_Src～PTS\_Dstに含まれるCMスキップ禁止箇所の過去の視聴回数が、制御回数1513以上である場合には、ステップS3006を実行する。

ステップS3005において、PTS\_Src～PTS\_Dstに含まれるCMスキップ禁止箇所の過去の視聴回数が、制御回数1513未満である場合には、ステップS3007を実行する。

#### 【0153】

コンテンツ利用制御部2106は、タイムスキップを実行する（ステップS3006）。具体的にはコンテンツ利用制御部2106は、指定されたスキップ先のTSパケット1400をコンテンツ蓄積部2103から取得するよう、コンテンツ復号部2107およびコンテンツ利用部2108を制御する。スキップ後の処理の動作は、図29で説明した動作と同様である。

#### 【0154】

コンテンツ利用制御部2106は、タイムスキップ動作を禁止する（ステップS3007）。具体的には、コンテンツ利用制御部2106は、タイムスキップ動作が不可である旨を（必要に応じてその理由とともに）、端末アプリケーション2111のユーザインターフェースを通じてユーザに通知する。

なお、ここではタイムスキップを行う場合の例を示したが、他の特殊再生の場合も同様の制御を行うことにより、CMなどコンテンツの特定箇所の特殊再生を防止することが可能である。

#### 【0155】

例えば、図31は、図28および図29で示した蓄積コンテンツの視聴中において、コンテンツの早送りを行う場合の動作を示すフローチャートである。

図31において、ユーザが端末アプリケーション2111を通じて再生中のコンテンツの早送りを要求すると、コンテンツ利用制御部2106は早送り指示を受信する（ステップS3101）。具体的には、コンテンツ利用制御部2106は、端末アプリケーション2111から早送りを示すアクションIDを受信する。

#### 【0156】

コンテンツ利用制御部2106は、ライセンス処理部2104から取得した再生制御情報に基づき、早送り（特殊再生）の制御期間内であるかどうかを判定する（ステップS3102）。具体的には、コンテンツ利用制御部2106は、再生制御情報（制御情報1503）の制御ID1511が「特殊再生不可」となっている情報を含む場合に、セキュアな計時部（図21に図示せず）から取得した日時情報と制御期限1512の値とを比較することにより、現在が特殊再生を制御すべき期間であるかどうかを判定する。

#### 【0157】

ステップS3102において、YESである場合、すなわち、現在が特殊再生を制御すべき期間である場合には、ステップS3103を実行する。

ステップS3102において、NOである場合、すなわち、現在が特殊再生を制御すべき期間でない場合には、ステップS3106を実行する。

コンテンツ利用制御部2106は、現在の再生箇所のPTS1343a（以下、PTS

Srcと記述)を取得する(ステップS3103)。具体的には、コンテンツ利用制御部2106は、コンテンツ利用部2108から現在再生している箇所のPTS1343a(最近に表示したフレームに付与されていたPTS1343a)を取得する。

#### 【0158】

コンテンツ利用制御部2106は、ライセンス処理部2104から取得した再生制御情報に基づき、早送り(特殊再生)を行える区間であるかどうかを判定する(ステップS3104)。具体的には、コンテンツ利用制御部2106は、再生制御情報(制御情報1503)の制御ID1511が「特殊再生不可」となっている情報を含む場合に、制御範囲1514で指定されるPTS1343aの範囲である制御開始時刻～制御終了時刻に、PTS\_Srcが含まれるかどうかを制御時刻個数1520の分だけチェックする。すなわち、現在再生している箇所が、少なくとも1つのCMスキップ禁止区間に(制御情報1503の制御開始時刻～制御終了時刻)包含される場合を検出している。

#### 【0159】

ステップS3104において、YESである場合、すなわち、PTS\_SrcがCMスキップ禁止箇所に含まれる場合は、ステップS3105を実行する。

ステップS3104において、NOである場合、すなわち、PTS\_SrcがCMスキップ禁止箇所に含まれない場合は、ステップS3106を実行する。

コンテンツ利用制御部2106は、当該コンテンツの視聴履歴を取得して、PTS\_Srcが含まれるCMスキップ禁止箇所の過去の視聴回数が、規定数以上であるかどうかを判定する(ステップS3105)。具体的には、コンテンツ利用制御部2106は、視聴履歴DB2106を検索して、視聴履歴DB2106に蓄積されたUL2200の内、コンテンツID2205が一致するUL2200の視聴履歴である時刻情報2210を参照する。時刻情報2210は、当該コンテンツを過去に視聴したPTS1343aの値が記載されているので、PTS\_Srcが含まれるCMスキップ禁止箇所を視聴した履歴数をカウントして、制御情報1503の制御回数1513と比較する処理を行う。

#### 【0160】

ステップS3105において、PTS\_Srcが含まれるCMスキップ禁止箇所の過去の視聴回数が、制御回数1513以上である場合には、ステップS3106を実行する。

ステップS3105において、PTS\_Srcが含まれるCMスキップ禁止箇所の過去の視聴回数が、制御回数1513未満である場合には、ステップS3107を実行する。

コンテンツ利用制御部2106は、早送りを実行する(ステップS3106)。具体的にはコンテンツ利用制御部2106は、早送りの速度に対応した分のTSパケット1400をコンテンツ蓄積部2103から取得するよう、コンテンツ復号部2107およびコンテンツ利用部2108を制御する。通常、早送りではMPEGのIピクチャのみを表示することが多いため、TSパケット1400のTSP\_Header1410やAdaptation\_Field1420の情報を参照しながら、IピクチャのみのTSパケット1400を選択する処理を行う。スキップ後の処理の動作は、図29で説明した動作と同様である。また、早送りにともなって変化する再生箇所が、CMスキップ禁止箇所か否かを逐次判定するため、ステップS3102～ステップS3106の処理を繰り返し実行する。なお、ステップS3102～ステップS3106の処理を繰り返し実行する際には、必要に応じて、ステップS3105の処理は省略しても可である。この場合、ステップS3105における処理は全てNOとして処理され、ステップS3107が実行される。

#### 【0161】

コンテンツ利用制御部2106は、早送り動作を禁止する(ステップS3107)。具体的には、コンテンツ利用制御部2106は、早送り動作が不可である旨を(必要に応じてその理由とともに)、端末アプリケーション2111のユーザインタフェースを通じてユーザに通知する。

このように、コンテンツの特定箇所に関して、期間限定かつ回数限定で該当部分の特殊再生を制御することができる。

#### 【0162】

さらに、本発明における実施の形態で述べた制御方法は、特殊再生の場合に限らず、コンテンツの特定部分の視聴を制御するという目的にも利用できる。この場合の例として、PPVコンテンツのプレビュー部分の視聴を制御する動作を、図32を用いて説明する。図32では、図30および図31と同様、コンテンツの視聴中において、コンテンツのプレビューを行う場合の動作を示すフローチャートである。

#### 【0163】

ユーザが端末アプリケーション2111を通じて、あるコンテンツのプレビュー再生を要求すると、コンテンツ利用制御部2106はプレビュー指示を受信する（ステップS3201）。具体的には、コンテンツ利用制御部2106は、端末アプリケーション2111からプレビューを示すアクションIDを受信する。

コンテンツ利用制御部2106は、ライセンス処理部2104から取得した再生制御情報に基づき、プレビューの制御期間内であるかどうかを判定する（ステップS3202）。具体的には、コンテンツ利用制御部2106は、再生制御情報（制御情報1503）の制御ID1511が「プレビュー可」となっている情報を含む場合に、セキュアな計時部（図21に図示せず）から取得した日時情報と制御期限1512の値とを比較することにより、現在がプレビューを実行可能な期間であるかどうかを判定する。

#### 【0164】

ステップS3202において、YESである場合、すなわち、現在がプレビューを実行可能な期間である場合には、ステップS3203を実行する。

ステップS3202において、NOである場合、すなわち、現在がプレビューを実行可能な期間でない場合には、ステップS3207を実行する。

コンテンツ利用制御部2106は、現在の再生箇所のPTS1343a（以下、PTS\_srcと記述）を取得する（ステップS3203）。具体的には、コンテンツ利用制御部2106は、コンテンツ利用部2108から現在再生している箇所のPTS1343a（最近に表示したフレームに付与されていたPTS1343a）を取得する。

#### 【0165】

コンテンツ利用制御部2106は、ライセンス処理部2104から取得した再生制御情報に基づき、プレビューが可能な区間であるかどうかを判定する（ステップS3204）。具体的には、コンテンツ利用制御部2106は、再生制御情報（制御情報1503）の制御ID1511が「プレビュー可」となっている情報を含む場合に、制御範囲1514で指定されるPTS1343aの範囲である制御開始時刻～制御終了時刻に、PTS\_srcが含まれるかどうかを制御時刻個数1520の分だけチェックする。すなわち、現在再生している箇所が、少なくとも1つのプレビュー可能区間に（制御情報1503の制御開始時刻～制御終了時刻）包含される場合を検出している。

#### 【0166】

ステップS3204において、YESである場合、すなわち、PTS\_srcがプレビュー可能区間に含まれる場合は、ステップS3205を実行する。

ステップS3204において、NOである場合、すなわち、PTS\_srcがプレビュー可能区間に含まれない場合は、ステップS3207を実行する。

コンテンツ利用制御部2106は、当該コンテンツの視聴履歴を取得して、PTS\_srcが含まれるプレビュー可能箇所の過去の視聴回数が、規定数以上であるかどうかを判定する（ステップS3205）。具体的には、コンテンツ利用制御部2106は、視聴履歴DB2106を検索して、視聴履歴DB2106に蓄積されたUL2200の内、コンテンツID2205が一致するUL2200の視聴履歴である時刻情報2210を参照する。時刻情報2210は、当該コンテンツを過去に視聴したPTS1343aの値が記載されているので、PTS\_srcが含まれるプレビュー可能箇所を視聴した履歴数をカウントして、制御情報1503の制御回数1513と比較する処理を行う。

#### 【0167】

ステップS3205において、PTS\_srcが含まれるプレビュー可能箇所の過去の視聴回数が、制御回数1513以上である場合には、ステップS3207を実行する。

ステップS3205において、PTS\_Srcが含まれるプレビュー可能箇所の過去の視聴回数が、制御回数1513未満である場合には、ステップS3206を実行する。

コンテンツ利用制御部2106は、プレビューを実行する（ステップS3206）。具体的にはコンテンツ利用制御部2106は、コンテンツのプレビューを許可し、コンテンツの復号およびコンテンツのデコードを実行する。また、プレビューにともなって再生箇所が変わっていくため、現在の再生箇所がプレビュー可能か否かを逐次判定するため、ステップS3202～ステップS3206の処理を繰り返し実行する。なお、ステップS3202～ステップS3206の処理を繰り返し実行する際には、必要に応じて、ステップS3205の処理は省略しても可である。この場合、ステップS3205における処理は全てYESとして処理され、ステップS3206が実行される。

#### 【0168】

コンテンツ利用制御部2106は、プレビューを禁止する（ステップS3207）。具体的には、コンテンツ利用制御部2106は、プレビューが不可である旨を（必要に応じてその理由とともに）、端末アプリケーション2111のユーザインタフェースを通じてユーザに通知する。

このように、PPVコンテンツのプレビューに関して、期間限定かつ回数限定でプレビューを制御することができる。

#### 【0169】

以上のように、コンテンツ利用制御システム1では、配信センター101が、コンテンツに付加した既存のセキュアな時刻情報を用いて、コンテンツの特定部分の利用を制御するための再生制御情報をコンテンツとは別データとしてセキュアに端末装置に配信するようになり、端末装置では、コンテンツに既存のセキュアな時刻情報と、配信センター101から取得した再生制御情報を用いて、コンテンツの利用をセキュアに制御するようにしている。そのため、事業者は、既存のエンコーダを活用することができ、送出設備に関するコストを軽減できるとともに、事業者が、ユーザによるコンテンツの特定部分の利用をセキュアに制御することが可能となる。

#### 【0170】

なお、本発明における実施の形態では、コンテンツに付加された時刻情報としてPESパケットのPTS1443aを用いる場合の例を示したが、これに限られるものではなく、PESパケットのDTS1443b、TSパケット1400のPCR1425a、MPEG-4 SystemsのSL(Sync Layer)、MPEG-2 ESのGroup Of PictureのTime Codeなど、コンテンツに既存の情報であり、かつ、コンテンツの部分を特定可能な情報を用いることが可能である。この場合、TSパケット1400のPCR1425aなど暗号化されない時刻情報を用いる場合は、時刻情報の値をコンテンツの暗号鍵に関連させるか、時刻情報の値を含むデータに対するハッシュ値を付加するなど、時刻情報をセキュアに配信するための処理が必要となる。

#### 【0171】

また、本発明における実施の形態では、MPEG-2 PES/TSで多重化されたコンテンツの例を示したが、MPEG-2 PS(Program Stream)やMPEG以外のコンテンツであっても、コンテンツに既存の情報であり、かつ、コンテンツの部分を特定可能な情報があれば適用することができると言うまでもない。

また、本発明における実施の形態では、ARIB STD-B25 4.1版に示されているサーバ型放送方式タイプIに基づいてコンテンツを配信する場合の例を示したが、ファイル型コンテンツの配信方式であるサーバ型放送方式タイプIIの場合や、インターネット上のストリーミング配信、ダウンロード配信などに適用可能であることは言うまでもない。この場合、一般的には、コンテンツは単一の暗号鍵Kc'で暗号化されるので、ライセンス（本発明における実施の形態におけるメインライセンス900に相当）に暗号鍵Kc'を設定し、ライセンスを権利管理サーバ101aからインターネットなどの通信経由で端末装置102に配信する。同様に、再生制御情報も、このライセンスに含める。このようにすることにより、コンテンツが時変鍵でスクランブルされておらず、単一の暗

号鍵で暗号化されている場合（すなわち、メインライセンス900とサブライセンス1000というライセンス構成ではなく、単一のライセンス構成の場合）においても、端末装置102でのコンテンツの特定部分の利用制御をセキュアに行うことができる。

#### 【0172】

また、本発明における実施の形態では、視聴履歴であるUL2200において、ユーザID2103や端末ID2104をはじめとする種々の情報を記録するようにしたが、視聴履歴に基づくコンテンツ利用制御に用いるためには、コンテンツとコンテンツの視聴箇所を特定することができれば良いため、コンテンツID2105またはライセンスID2106、あるいはコンテンツID2105かつライセンスID2106（コンテンツ利用制御システム1内におけるIDの割り当てかたに依存する）と、1以上の開始時刻情報と終了時刻情報の組を記録すれば良い。

#### 【0173】

また、本発明における実施の形態では、端末装置102において記録した視聴履歴を、視聴履歴DB2110で管理する場合の例を示したが、ライセンスDB2105において管理されるライセンス（メインライセンス900）とともに管理するようにしても良い。

また、本発明における実施の形態では、コンテンツの特定箇所の利用制御を行う場合の例としてCMスキップ制御を行う場合の例を示したが、これに限られるものではなく、例えば、ダイジェスト視聴のような、コンテンツの特定箇所だけを利用させるような制御にも適用できる。

#### 【0174】

また、本発明における実施の形態では、再生制御情報における再生制御箇所の情報（制御情報1545）として、コンテンツに付与されたPTS1343aの値そのものを用いて指定する場合の例を示したが、コンテンツの先頭でのPTS1343aの値と、PTS1343aに基づくコンテンツの先頭からの相対値とを用いて、制御情報1545を構成するようにしても良い。また、制御情報1545において、再生制御箇所を制御開始時刻と制御終了時刻とで指定された範囲で表現したが、制御開始時刻と制御時間（時間幅）という表現にしても良い。

#### 【0175】

また、本発明における実施の形態では、再生制御情報における再生制御箇所の情報（制御情報1545）として、特殊再生禁止区間（通常再生のみを許可する区間）を記述する場合の例を示したが、制御情報1545に特殊再生許可区間を記述するようにしても良い。

また、本発明における実施の形態では、再生制御情報をライセンス（サブライセンス1000）、ECMに設定して、配信センター101から端末装置102に配信する場合の例を示したが、これに限られるものではなく、通信でSSLなどのセキュアなチャネルを用いて配信したり、放送でのEMMで配信したりするようにしても良い。よって本方式は、コンテンツへのECMなどの関連情報の多重化有無にかかわらず、統一的に適用可能な方式である。なお、このような場合、コンテンツ利用時点で端末装置102が再生制御情報（制御情報1545）を取得していない場合には、当該コンテンツの視聴においては通常再生しか許可しない、または、プレビューを許可しないように制御し、再生制御情報を取得後に特殊再生やプレビューなどを許可するように制御しても良い。

#### 【0176】

また、コンテンツの先頭でのPTS1343aの値と、PTS1343aに基づくコンテンツの先頭からの相対値とを用いて制御情報1545が構成される場合、コンテンツ配信サーバ101bにおけるストリーミングコンテンツの送出時にPTS1343aに基づくコンテンツの先頭からの相対値で再生制御箇所を指定しておき、コンテンツの先頭のPTS1343aが確定した後に、コンテンツの先頭のPTS1343aをコンテンツ配信サーバ101bから端末装置102に配信するようにしても良い。このとき、端末装置102がコンテンツの先頭のPTS1343aを取得していない間は、通常再生しか許可しない、または、プレビューを許可しないように制御する。

**【0177】**

また、本発明における実施の形態では、ライセンス（サプライセンス1000）をKc配信用ECM1900に設定して、配信センター101から端末装置102に配信する場合の例を示したが、これに限られるものではなく、ECM-Kw1800、ECM-Kc1810や、EMM（サーバ型放送方式タイプIでのKc配信用EMMも含む）で配信するようにしても良い。また、放送による配信では、ECM-Kw1800、ECM-Kc1810を用い（必要に応じて、ワーク鍵Kw203の配信のためのEMMを用いても良い）、コンテンツ鍵Kc205および再生制御情報を含むライセンスを、通信経由で配信するようにしても良い。

**【0178】**

また、本発明における実施の形態では、コンテンツの特定箇所の利用を制御する制御情報の例として、再生制御のための情報（再生制御情報）を配信する場合の例を示したが、これに限られるものではなく、印刷や編集など、端末装置102における再生以外の利用制御についても適用可能である。

また、本発明における実施の形態では、コンテンツ配信サーバ101bにおいて再生制御情報を生成する場合の例を示したが、権利管理サーバ101aで生成するようにしても良い。この場合、コンテンツに付与されるPTS1343aの情報をコンテンツ配信サーバ101bから権利管理サーバ101aに通知する必要があることは言うまでもない。また、コンテンツ配信サーバ101bにおいて、サプライセンス1000に再生制御情報を設定するようにしたが、権利管理サーバ101bで設定するようにしても良い。

**【0179】**

また、本発明における実施の形態では、端末装置102において、全てのコンテンツ利用に対する視聴履歴を記録する場合の例を示したが、メインライセンス900あるいはサプライセンス1000に視聴履歴の記録を指示する情報を含めておくことにより、これに従ってコンテンツ毎やライセンス毎、あるいは、ユーザ毎に視聴履歴を記録するかどうかの制御を行うようにしても良い。

**【0180】**

また、本発明における実施の形態では、コンテンツ配信サーバ101bにおける再生制御情報生成部1106が、再生制御情報の生成にあたりコンテンツ符号化部1105からPTS1343aの値を取得する場合の例を示したが、時刻情報付加部1104からSTCの値を直接取得するようにしても良い。但し、この場合、コンテンツ符号化部1105が用いるSTCの値と、再生制御情報生成部1106が用いるSTCの値は一致する必要があることは言うまでもない。

**【0181】**

また、本発明における実施の形態では、コンテンツ配信サーバ101bにおける再生制御情報生成部1106が、ストリーミングコンテンツ（リアルタイムエンコード）する場合において、コンテンツの先頭のPTS1343aの値を算出して、再生制御情報を生成する場合の例を示したが、ダウンロードコンテンツ（プリエンコード）する場合においては、予めコンテンツのコンテンツ先頭のPTS1343aの値や、CM箇所、プレビュー可能箇所などのPTS1343aの値を特定することができるため、実際にコンテンツに付加されたPTS1343aの値に基づき、再生制御情報を生成することが可能である。

**【0182】**

また、本発明における実施の形態では、再生制御情報（制御情報1503）の制御ID1511として、「特殊再生不可」、「プレビュー可」というIDを用いる場合の例を示したが、端末装置102におけるユーザの操作やコンテンツの処理を規定するための識別子であれば、これに限られるものではない。

また、本発明における実施の形態では、制御ID1511に対して視聴履歴に基づく過去の視聴回数や、絶対時刻により制御期限などの制約が加えられている場合の例を示したが、過去の視聴時間などの制約を加えるようにしても良い。

**【0183】**

また、本発明における実施の形態では、視聴履歴DB2110に蓄積された視聴履歴を用いて、コンテンツの特定箇所の再生制御を行う場合の例を示したが、視聴履歴に基づき再生制御情報（制御情報1545）を変更するようにしても良い。例えば、特殊再生禁止区間を規定回数以上視聴した場合は、制御情報1545から該当の特殊再生禁止区間の情報を削除する。これにより、視聴履歴を配信センター101などに送信した後であっても、視聴履歴に基づく再生制御が可能となる。

#### 【0184】

また、本発明における実施の形態では、再生制御情報をKc配信用ECM1900に設定する場合の例を示したが、ECM-Kw1800やECM-Kc1810に設定するようにしても良い。このとき、ECM-Kw1800とECM-Kc1810、または、ECM-Kw1800とKc配信用ECM1900に異なる再生制御情報を設定するようすれば、リアルタイム視聴時と蓄積視聴時で異なる再生制御範囲が実現できる。例えば、プレビューの場合は、リアルタイム視聴時は先頭から一定時間といった画一的なレビュー区間とならざるを得ないが、蓄積視聴時はダイジェスト視聴のようなコンテンツの特徴を生かしたレビュー範囲を設定することができ、端末機能102の蓄積機能を十分に生かしたサービス提供が可能となる。

#### 【0185】

さらに、本発明における実施の形態では、単一の配信経路からコンテンツやライセンス、制御情報などを取得する場合の例を示したが、デジタル放送とインターネットを併用したり、パッケージメディアとインターネットを併用したりといった、複合的な配信経路から取り込むようにすることもできる。

#### 【産業上の利用可能性】

#### 【0186】

本発明にかかるコンテンツ利用制御システムは、コンテンツに制御情報を追加することなく、コンテンツに既存のセキュアな時刻情報を用いて、端末装置でのコンテンツのCM部分などのコンテンツの特定部分の利用制御をセキュアに実現することにより、低廉なコストで事業者の意図に反するユーザのコンテンツ利用を防止できるという効果を有し、デジタル放送、CATV、インターネットなどによるコンテンツ配信サービスにおけるコンテンツ利用制御システムなどとして有用である。またパッケージメディアなどの可搬メディアなどによるコンテンツ配信サービスにおけるコンテンツ利用制御システムにも応用できる。

#### 【図面の簡単な説明】

#### 【0187】

【図1】本発明の実施の形態に係るコンテンツ利用制御システム1の全体の概略構成を示す図

【図2】本発明の実施の形態に係る暗号鍵スキームの概要を示す図

【図3】本発明の実施の形態に係る権利管理サーバ101aの構成を示す機能プロック図

【図4】本発明の実施の形態に係る鍵情報DB301のワーク鍵管理テーブルの構成を示す図

【図5】本発明の実施の形態に係る鍵情報DB301のコンテンツ鍵管理テーブルの構成を示す図

【図6】本発明の実施の形態に係るユーザ情報DB302のテーブル構成を示す図

【図7】本発明の実施の形態に係る利用条件DB303のテーブル構成を示す図

【図8】本発明の実施の形態に係るコンテンツ情報DB304のテーブル構成を示す図

【図9】本発明の実施の形態に係るメインライセンス900の構成を示す図

【図10】本発明の実施の形態に係るサプライセンス1000の構成を示す図

【図11】本発明の実施の形態に係るコンテンツ配信サーバ101bの構成を示す機能プロック図

【図12】本発明の実施の形態に係るコンテンツ属性情報DB1102のテーブル構成を示す図

【図13】本発明の実施の形態に係るPESパケット1300の概略構成を示す図

【図14】本発明の実施の形態に係るTSパケット1400の概略構成を示す図

【図15】本発明の実施の形態に係る制御情報タグロック1500の構成を示す図

【図16】本発明の実施の形態に係るコンテンツ送出開始時のPTS1343aを算出する方法の概略を示す図

【図17】本発明の実施の形態に係る制御情報1503の一例を示す図

【図18】本発明の実施の形態に係るECM-Kw1800、ECM-Kc1810の構成を示す図

【図19】本発明の実施の形態に係るKc配布用ECM1900の構成を示す図

【図20】本発明の実施の形態に係る制御情報タグロック1500挿入後のサプライセンス1000の構成を示す図

【図21】本発明の実施の形態に係る端末装置102の構成を示す図

【図22】本発明の実施の形態に係るUL2200の構成を示す図

【図23】本発明の実施の形態に係るELI2300の構成を示す図

【図24】本発明の実施の形態に係る端末装置102における権利管理サーバ101aからのメインライセンス900の取得処理を示すフローチャート

【図25】本発明の実施の形態に係る権利管理サーバ101aにおけるライセンス発行可否判定処理を示すフローチャート

【図26】本発明の実施の形態に係る権利管理サーバ101aにおけるサプライセンス1000を生成する処理、および、ワーク鍵Kw203、コンテンツ鍵Kc205、サプライセンス1000を送信する処理を示すフローチャート

【図27】本発明の実施の形態に係るコンテンツ配信サーバ101bにおけるECM生成処理、および、コンテンツ送出処理を示すフローチャート

【図28】本発明の実施の形態に係る端末装置102におけるコンテンツ利用処理、および、ライセンス利用判定処理を示すフローチャート

【図29】本発明の実施の形態に係る端末装置102におけるコンテンツ利用処理を示すフローチャート

【図30】本発明の実施の形態に係る端末装置102におけるCM部分のタイムスカップ制御処理を示すフローチャート

【図31】本発明の実施の形態に係る端末装置102におけるCM部分の早送り制御処理を示すフローチャート

【図32】本発明の実施の形態に係る端末装置102におけるプレビュー制御処理を示すフローチャート

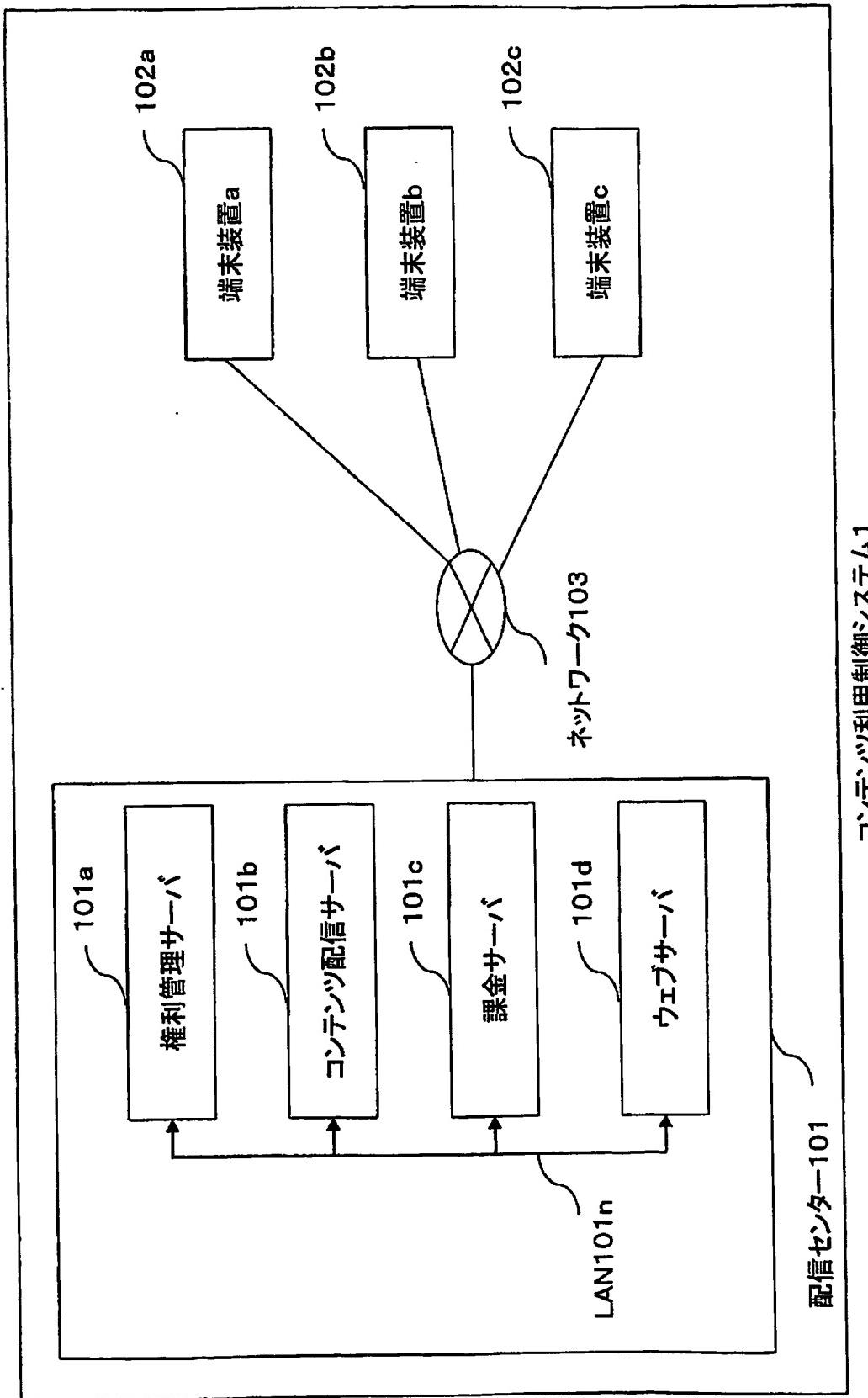
#### 【符号の説明】

##### 【0188】

- 1 コンテンツ利用制御システム
- 101 配信センター
- 101a 権利管理サーバ
- 101b コンテンツ配信サーバ
- 101c 課金サーバ
- 101d ウェブサーバ
- 101n LAN
- 102 端末装置
- 103 ネットワーク
- 201 スクランブル鍵Ks
- 205 コンテンツ鍵Kc
- 203 ワーク鍵Kw
- 301 鍵情報DB

302 ユーザ情報DB  
303 利用条件DB  
304 コンテンツ情報DB  
311 ライセンス発行部  
312 サーバ送受信部  
1101 コンテンツDB  
1102 コンテンツ属性情報DB  
1103 計時部  
1104 時刻情報付加部  
1105 コンテンツ符号化部  
1106 再生制御情報生成部  
1107 ECM生成部  
1108 コンテンツ多重化部  
1109 コンテンツ暗号化部  
1110 コンテンツ送出部  
2101 端末送受信部  
2102 分離部  
2103 コンテンツ蓄積部  
2104 ライセンス処理部  
2105 ライセンスDB  
2106 コンテンツ利用制御部  
2107 コンテンツ復号部  
2108 コンテンツ利用部  
2109 視聴履歴記録部  
2110 視聴履歴DB

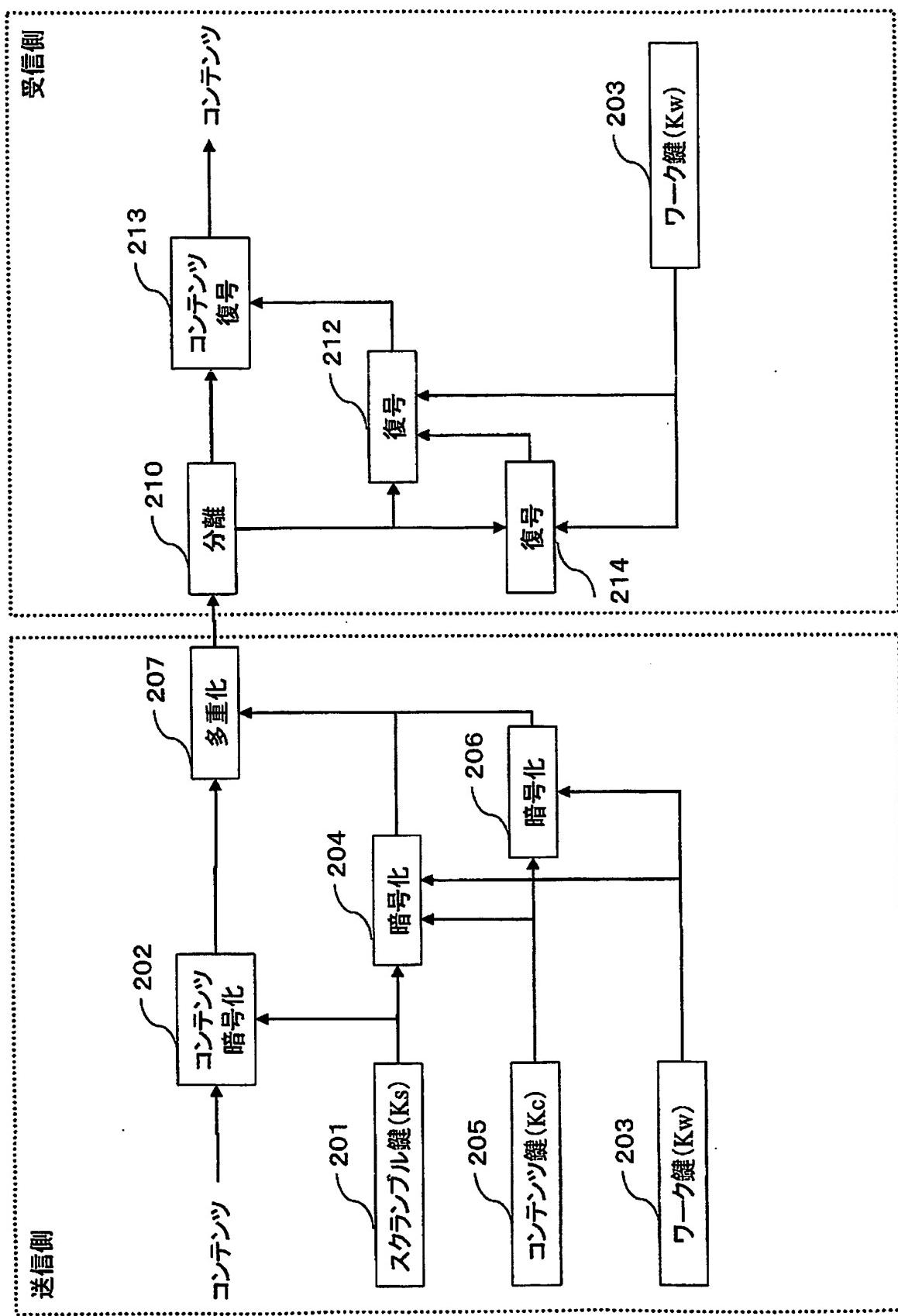
【書類名】 図面  
【図 1】



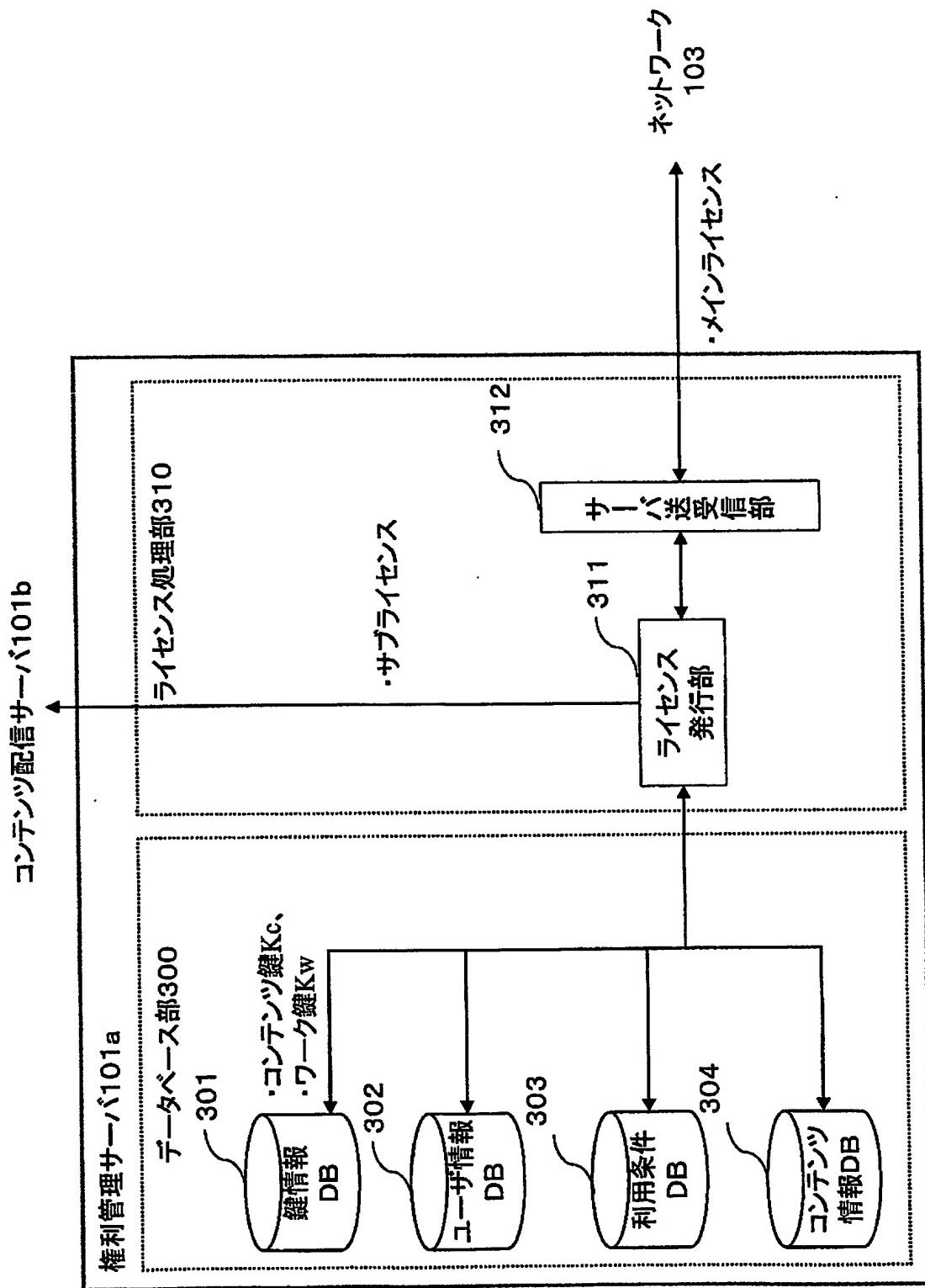
コンテンツ利用制御システム1

配信センター-101

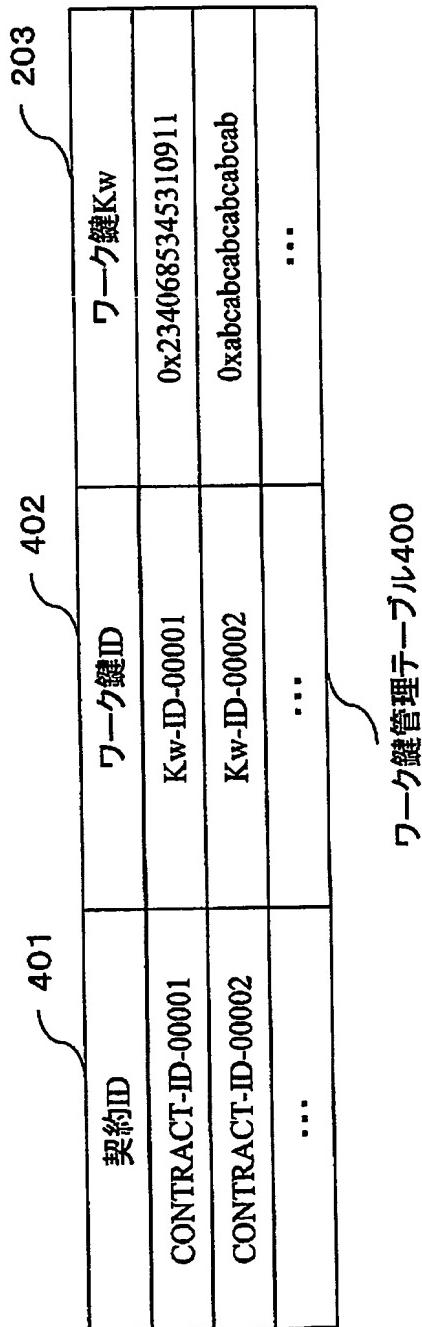
【図 2】



【図3】



【図 4】



【図5】

コンテンツID	コンテンツ鍵Kc
CONTENT-ID-00001	0x1234567890abcdef
CONTENT-ID-00002	0x43195745a4098b4e
CONTENT-ID-00003	0x3970584ad3922247
CONTENT-ID-00004	0x2411197120121974
...	...

コンテンツ鍵管理テーブル500

【図6】

ユーザID	端末ID
USER-ID-00001	TERMINAL-ID-00001
USER-ID-00002	TERMINAL-ID-12345 TERMINAL-ID-54321
USER-ID-00003	TERMINAL-ID-77777
USER-ID-00004	TERMINAL-ID-99999
...	...

ユーザ情報管理テーブル600

【図7】

ユーザーID	利用条件ID	契約ID	有効期間	発行可能残回数
USER-ID-00001	URUs-ID-00001	CONTRACT-ID-00001	2002/12/31～2003/1/30	1
USER-ID-00002	URUs-ID-00002	CONTRACT-ID-13452	2002/12/1～2002/12/31	1
USER-ID-00002	URUs-ID-10011	CONTRACT-ID-99999	∞	3
USER-ID-00003	URUs-ID-24024	CONTRACT-ID-02804	2002/11/24～2002/12/23	2
...	...	...	...	...

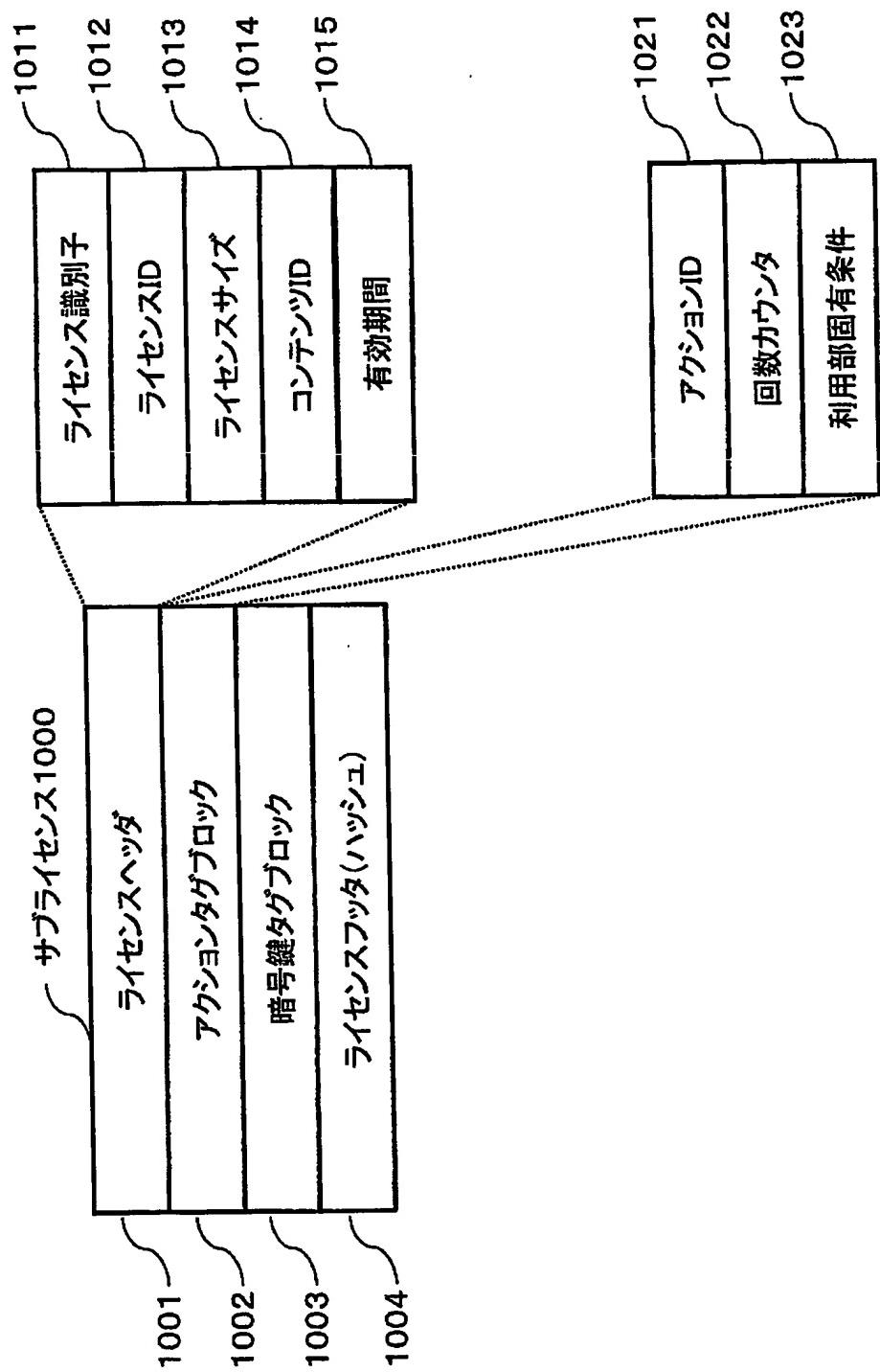
利用条件管理テーブル700

【図8】

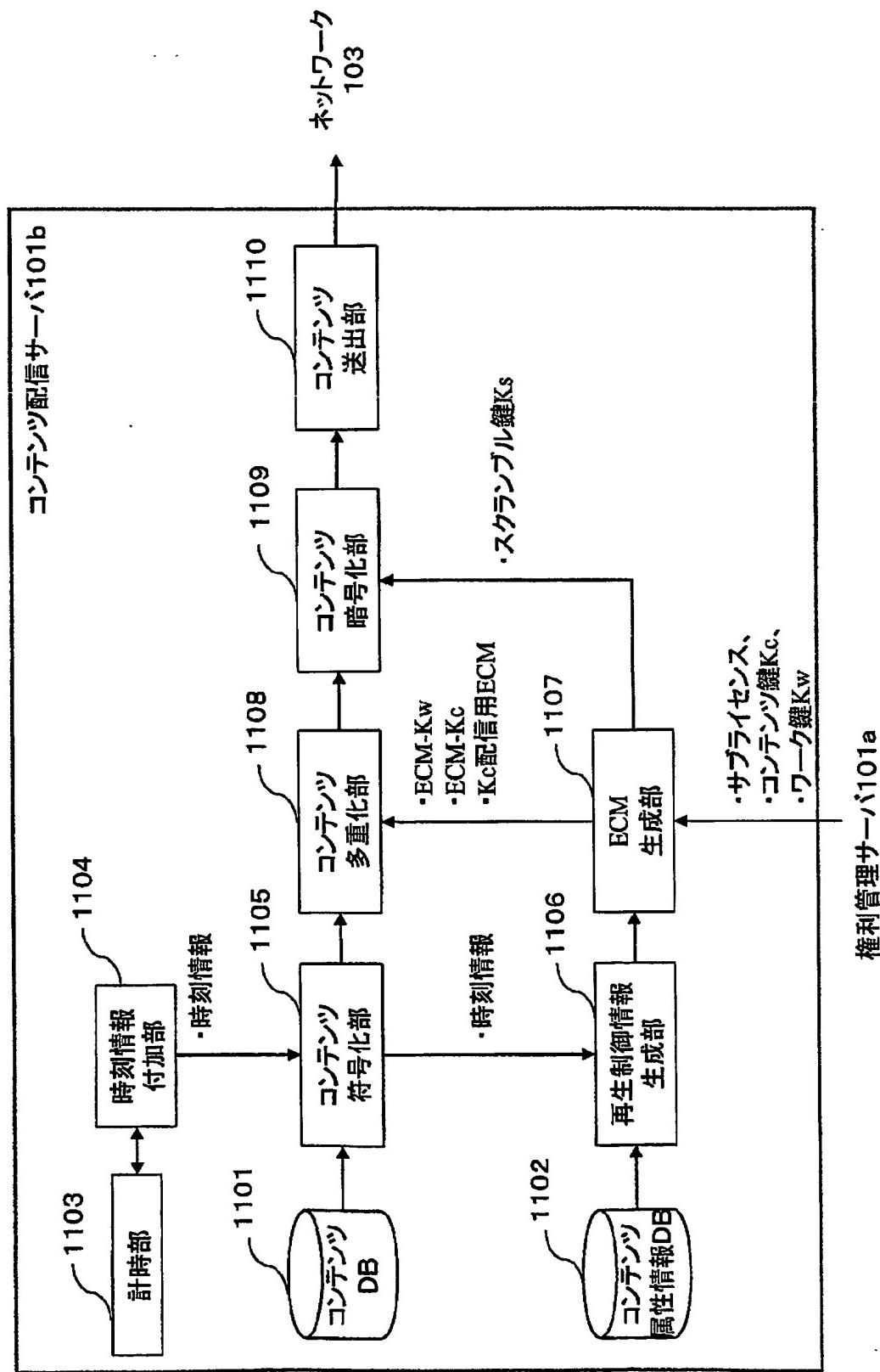
コンテンツID	ライセンスID	有効期間	利用可能回数
CONTENT-ID-00001	LICENSE-ID-00001	2003/12/31～2004/1/30	∞
CONTENT-ID-00002	LICENSE-ID-00002	2003/12/1～2004/12/31	∞
CONTENT-ID-00003	LICENSE-ID-00003	∞	1
CONTENT-ID-00004	LICENSE-ID-00004	2003/11/24～2004/12/23	5
...	...	...	...

コンテンツ情報管理テーブル800

【図10】



### 【図 1 1】



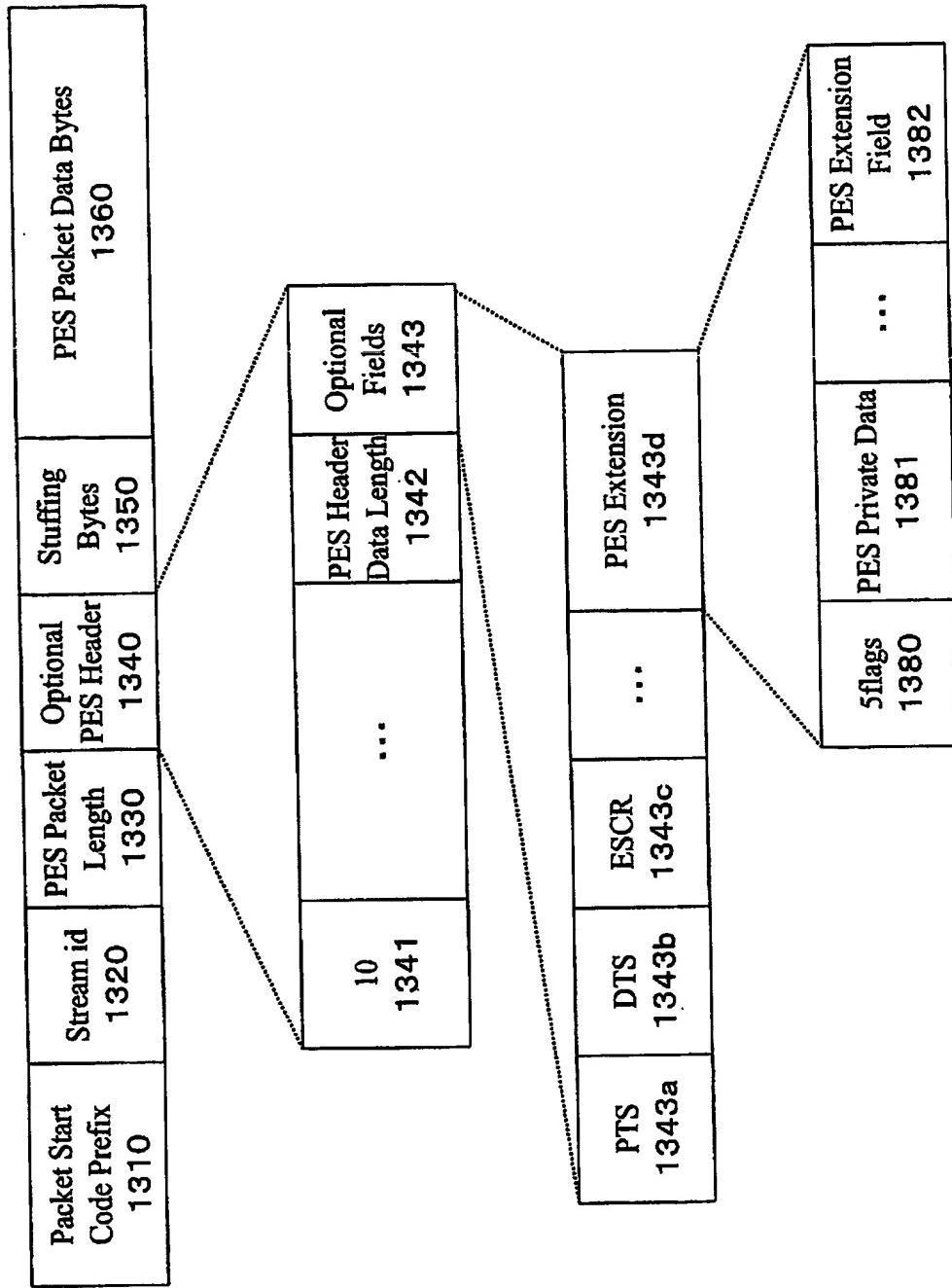
【図12】

コンテンツID	コンテンツ名称	プレビュー可能区間	CM区間	...
CONTENT-ID-00001	井上哲也NEWS23	0分～10分 ...	5分～8分 20分～25分 40分～43分 ...	...
CONTENT-ID-00002	プロダクトX	リアルタイム: 0分～10分 蓄積: 5分～10分: 20分～30分: ...	— ...	...
...	...	...	...	...

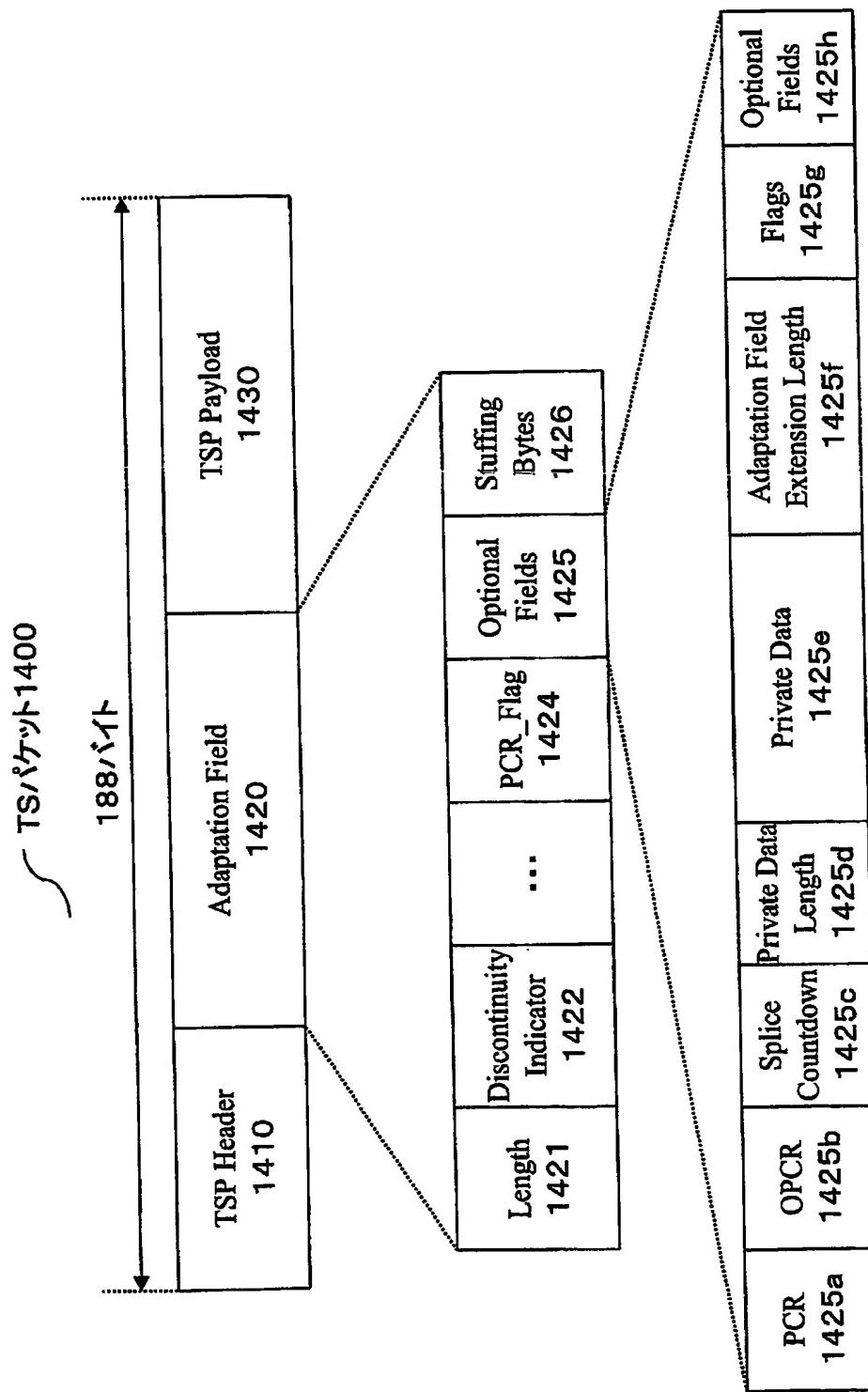
コンテンツ属性情報管理テーブル1200

【図 13】

PES/パケット1300

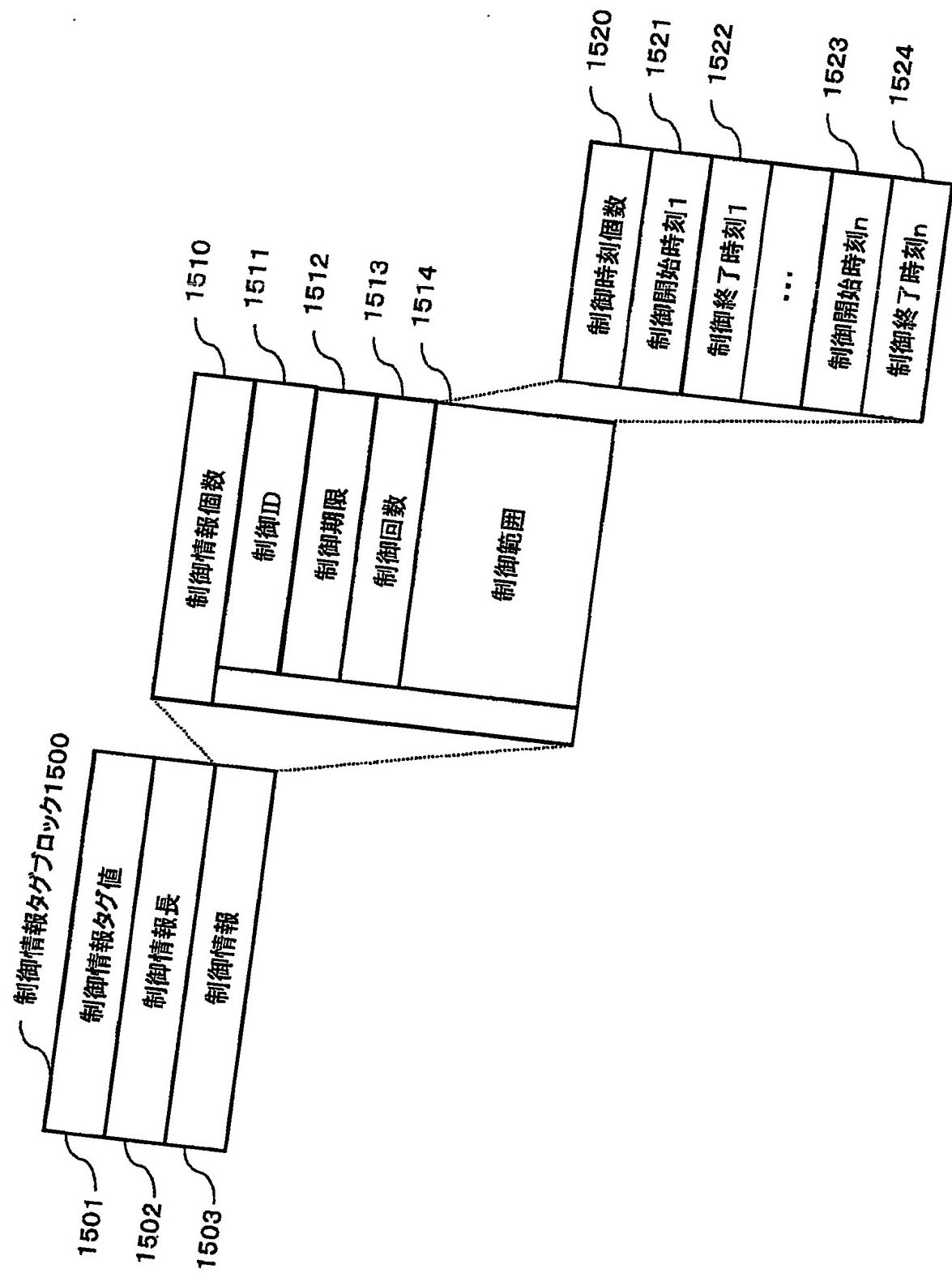


【図14】

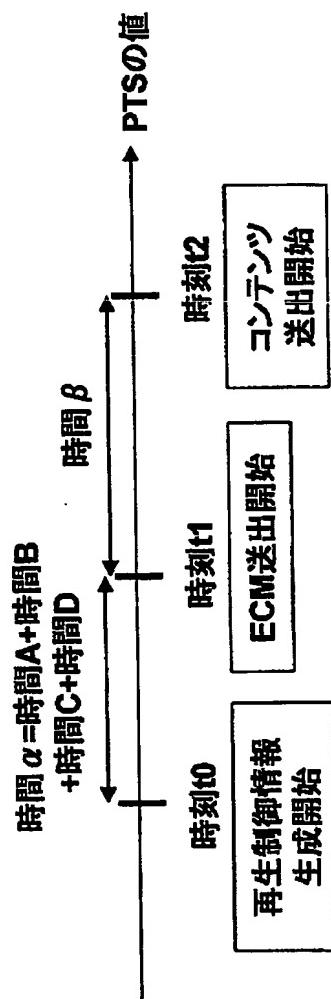


特願2003-378574

【図15】



【図16】

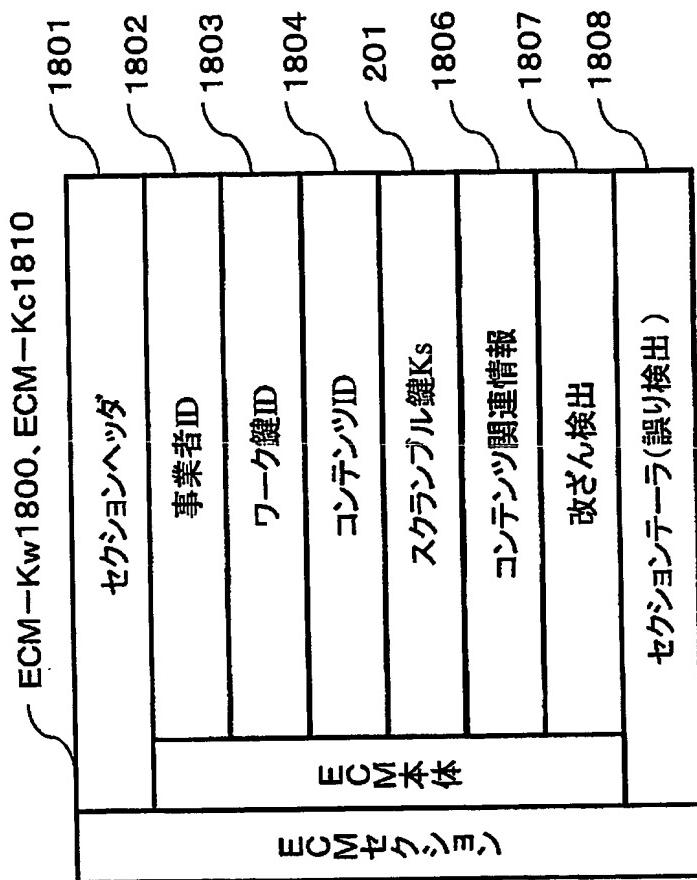


【図17】

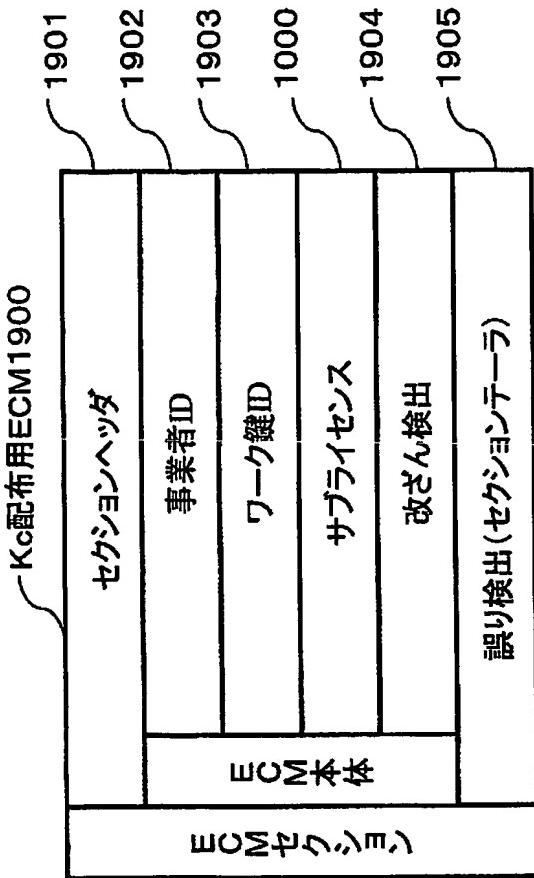
2	1701
プレビュー可	1702
2004/9/14	1703
1回	1704
10000	1705
100000	1706
特殊再生不可	1711
2004/7/6	1712
3回	1713
20000	1714
100000	1715
500000	1716
1000000	1717
...	

制御情報1503

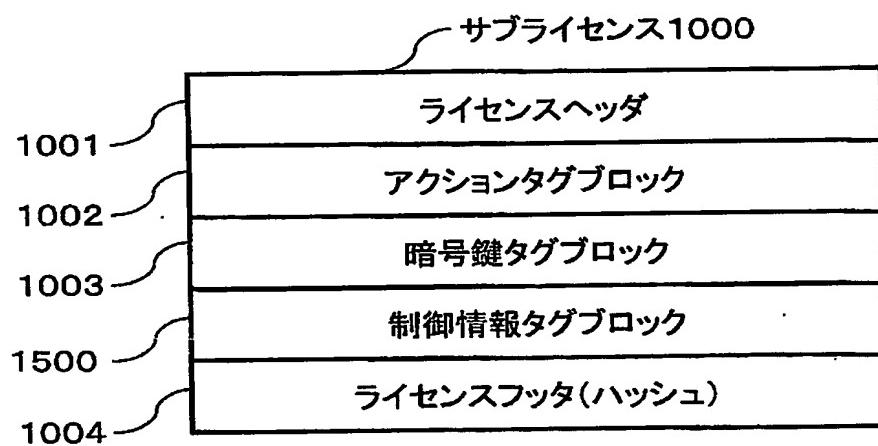
【図18】



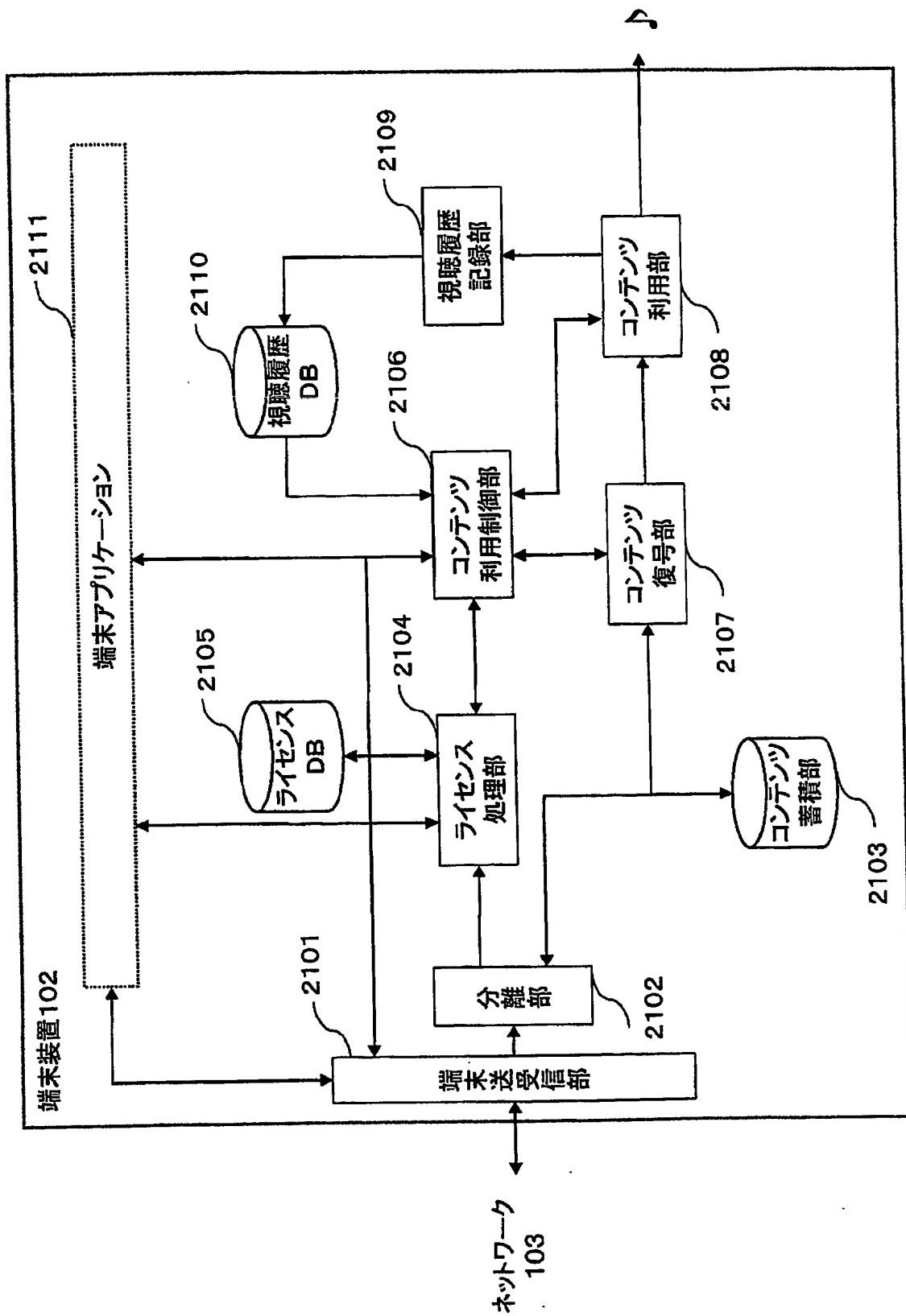
【図19】



【図20】



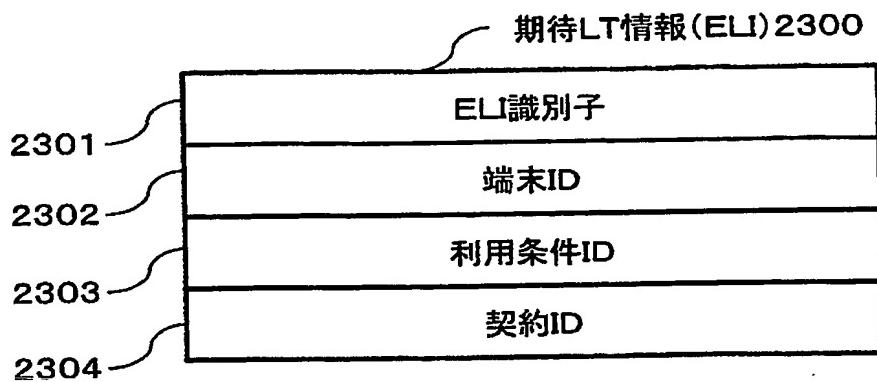
【図21】



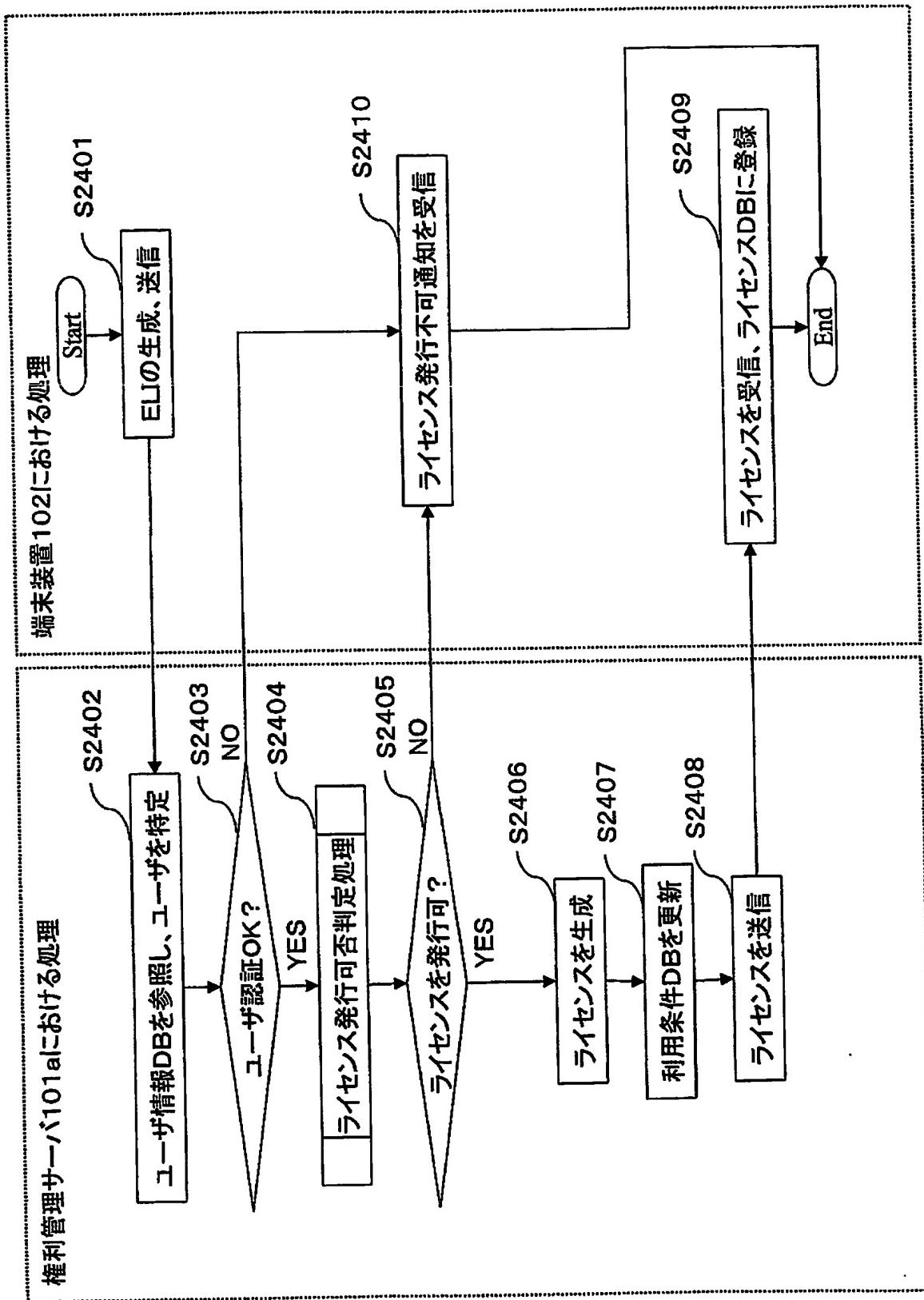
【図22】

		XDRM-UL
2201	UL識別子	
2202	ULサイズ	128
2203	ユーザID	USER-ID-00001
2204	端末ID	TERMINAL-ID-00001
2205	コンテンツID	CONTENT-ID-00001
2206	ライセンスID	LICENSE-ID-223606
2207	アクション種別	Play
2208	利用開始時刻	2003/1/1 10:00:00
2209	時刻情報個数	5
2210	時刻情報	13970584 1399999 ... 32141683 39705843970

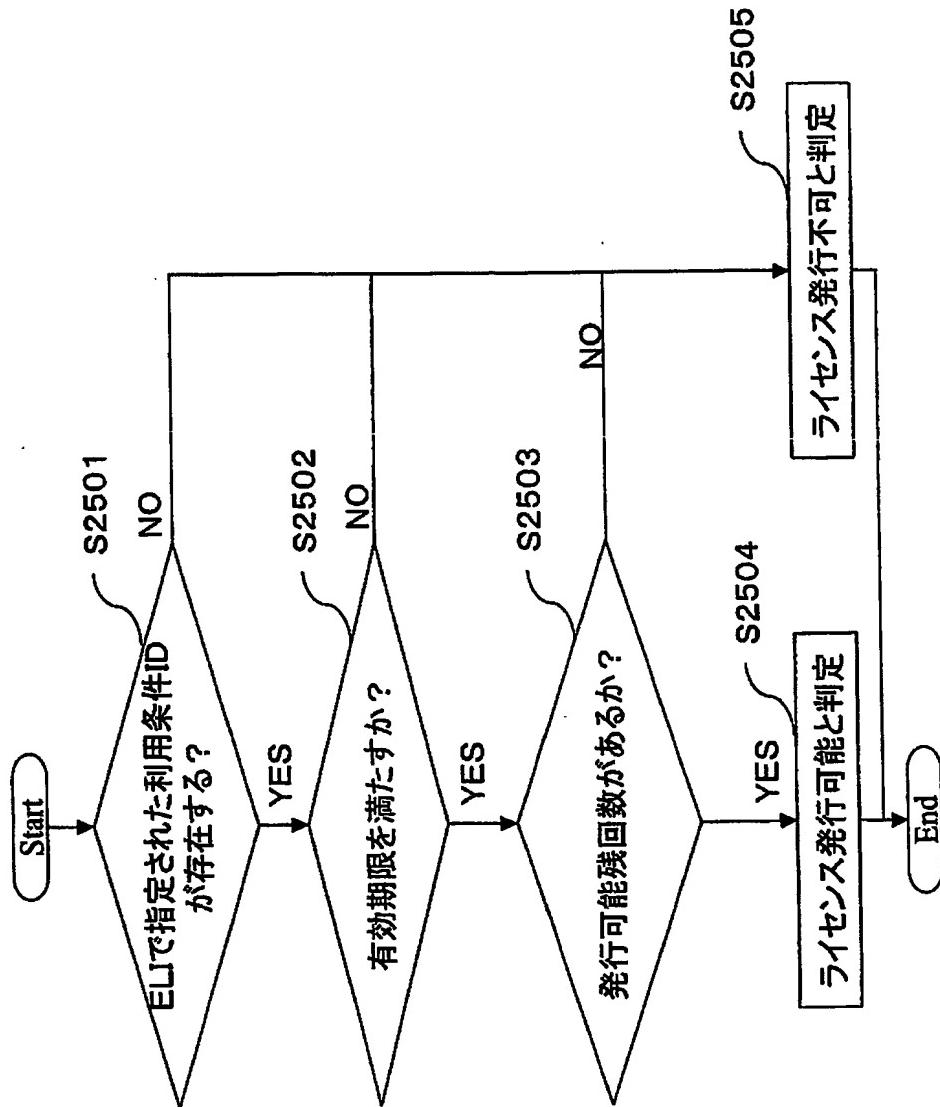
【図23】



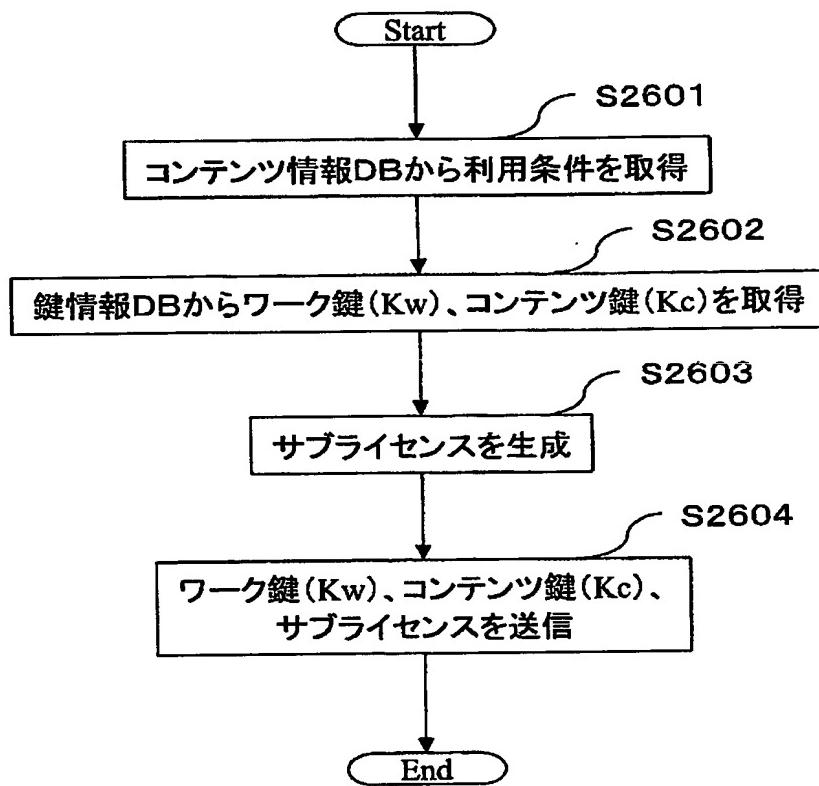
【図24】



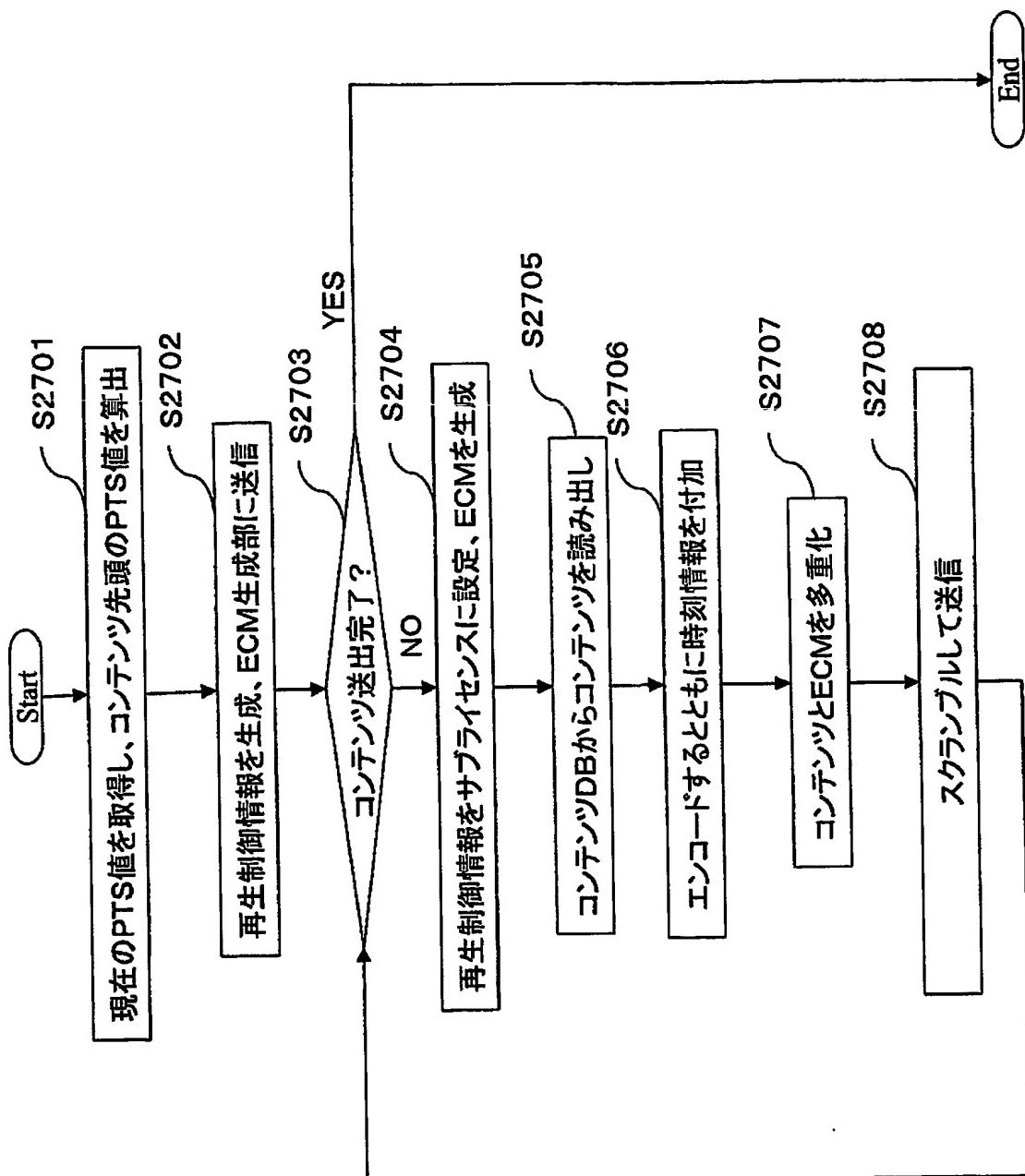
【図25】



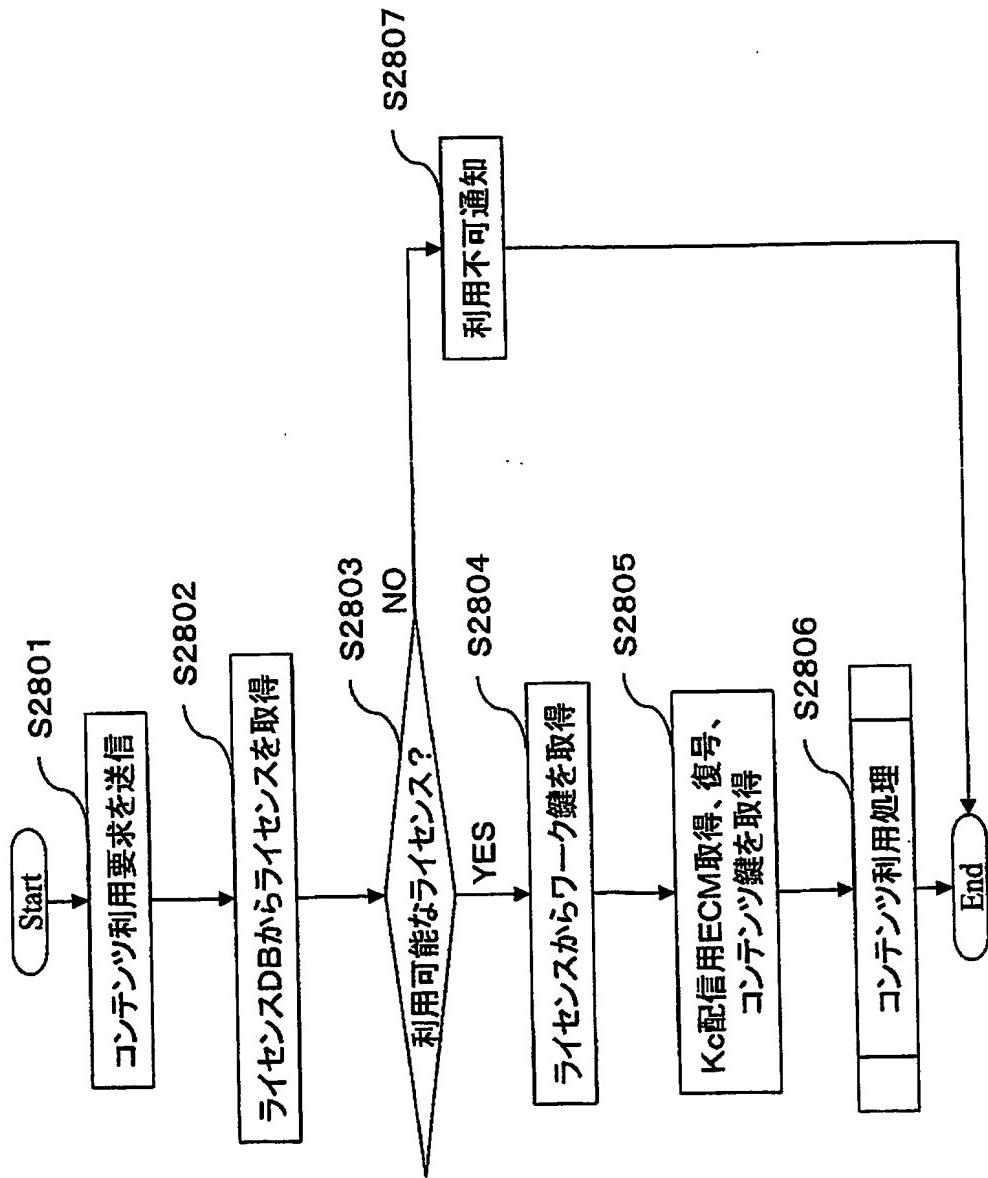
【図26】



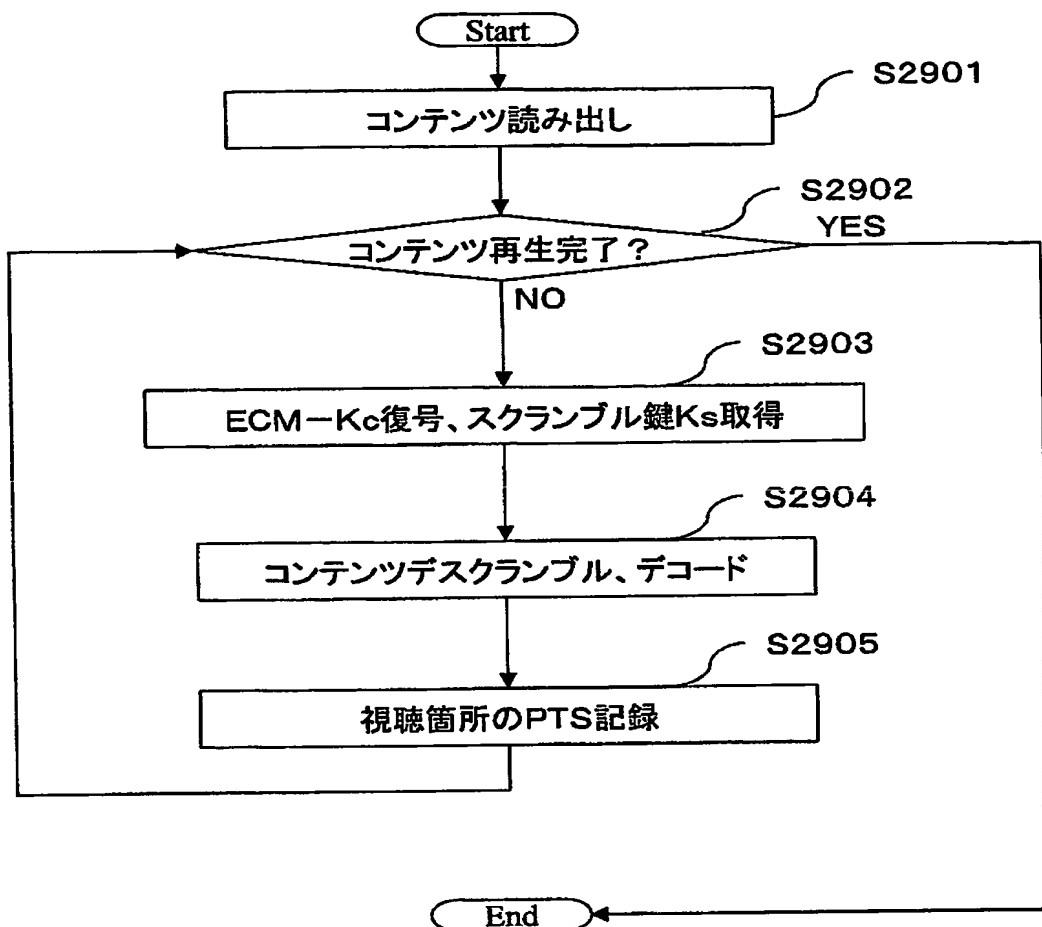
【図27】



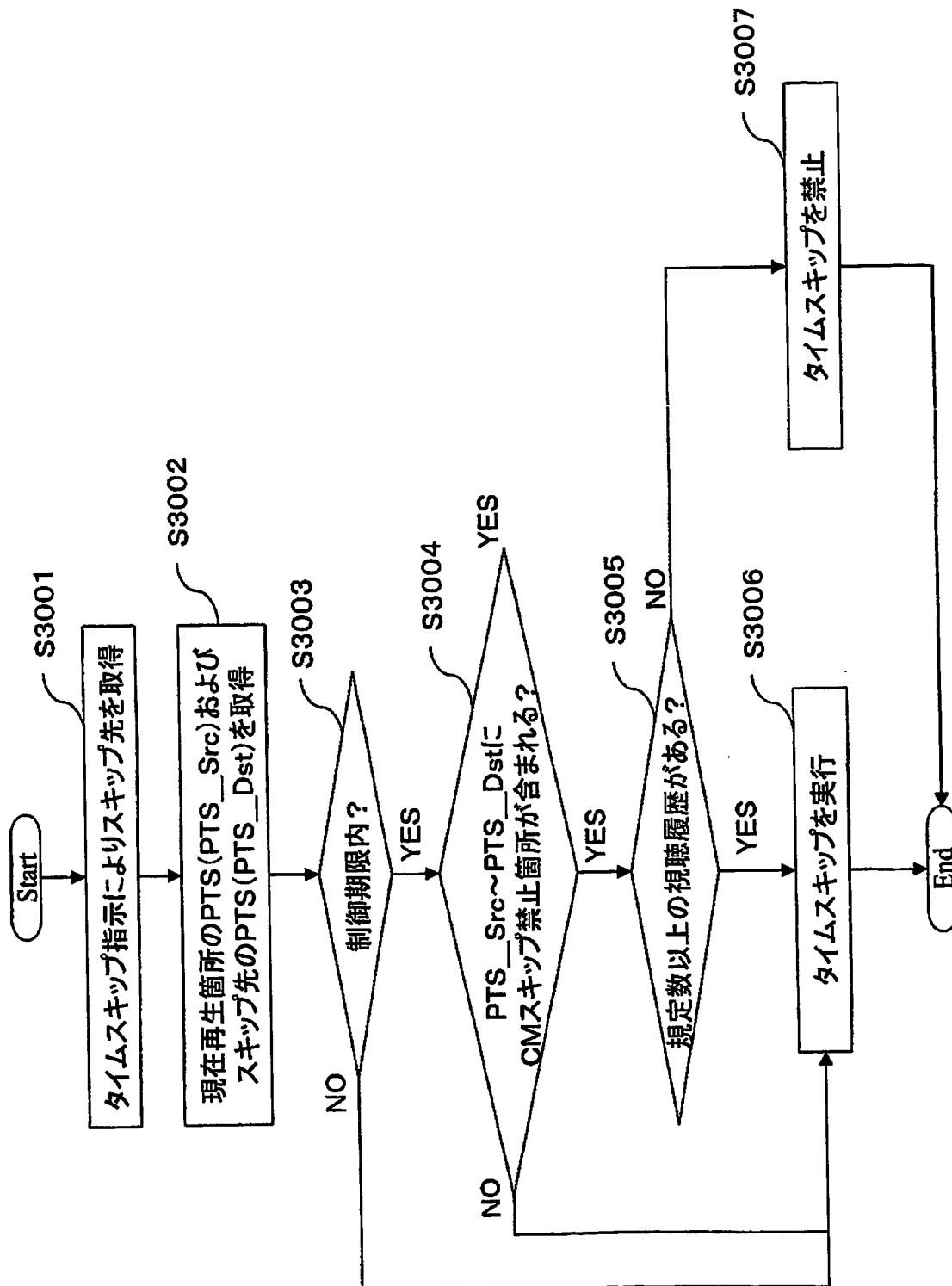
【図28】



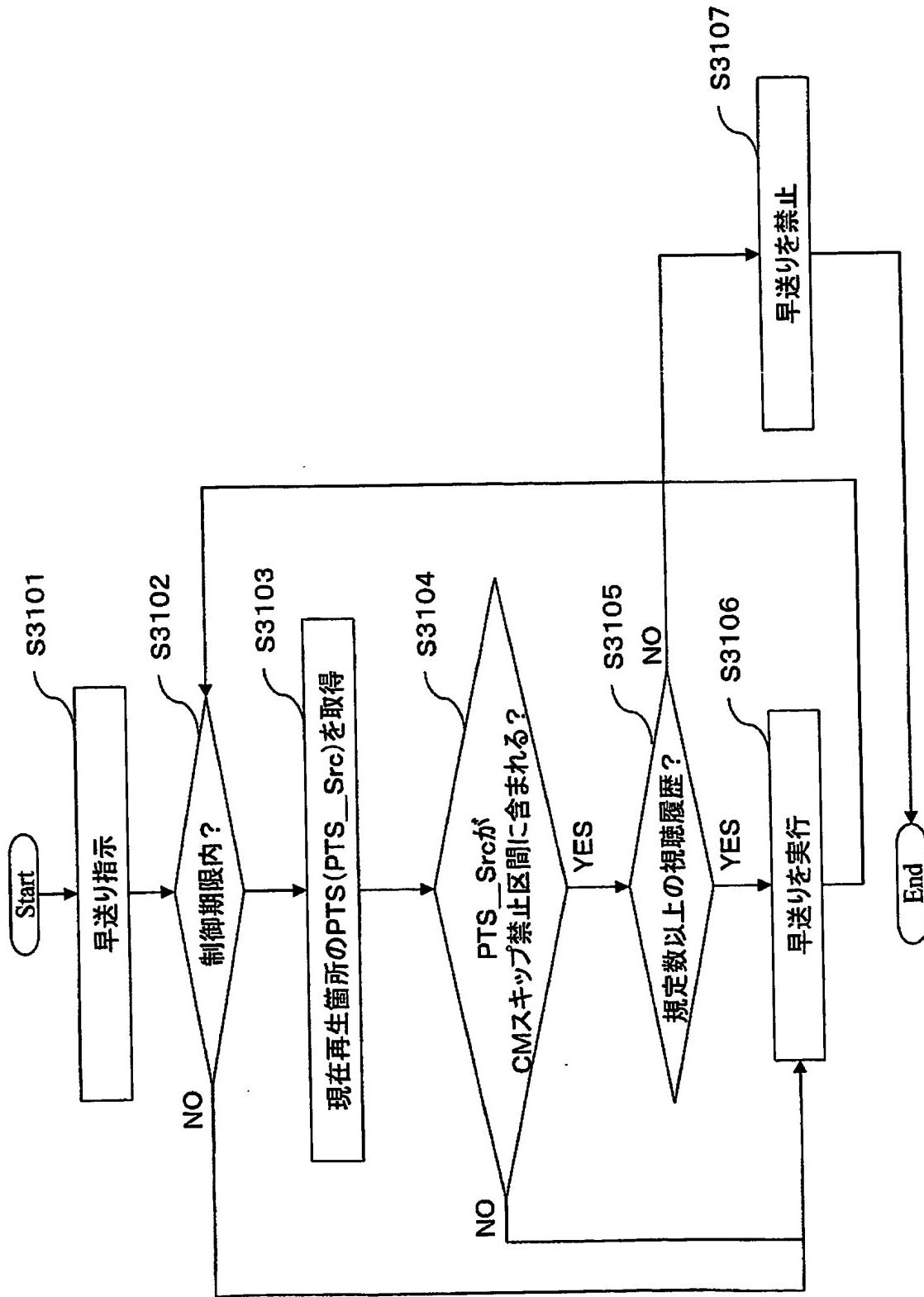
【図29】



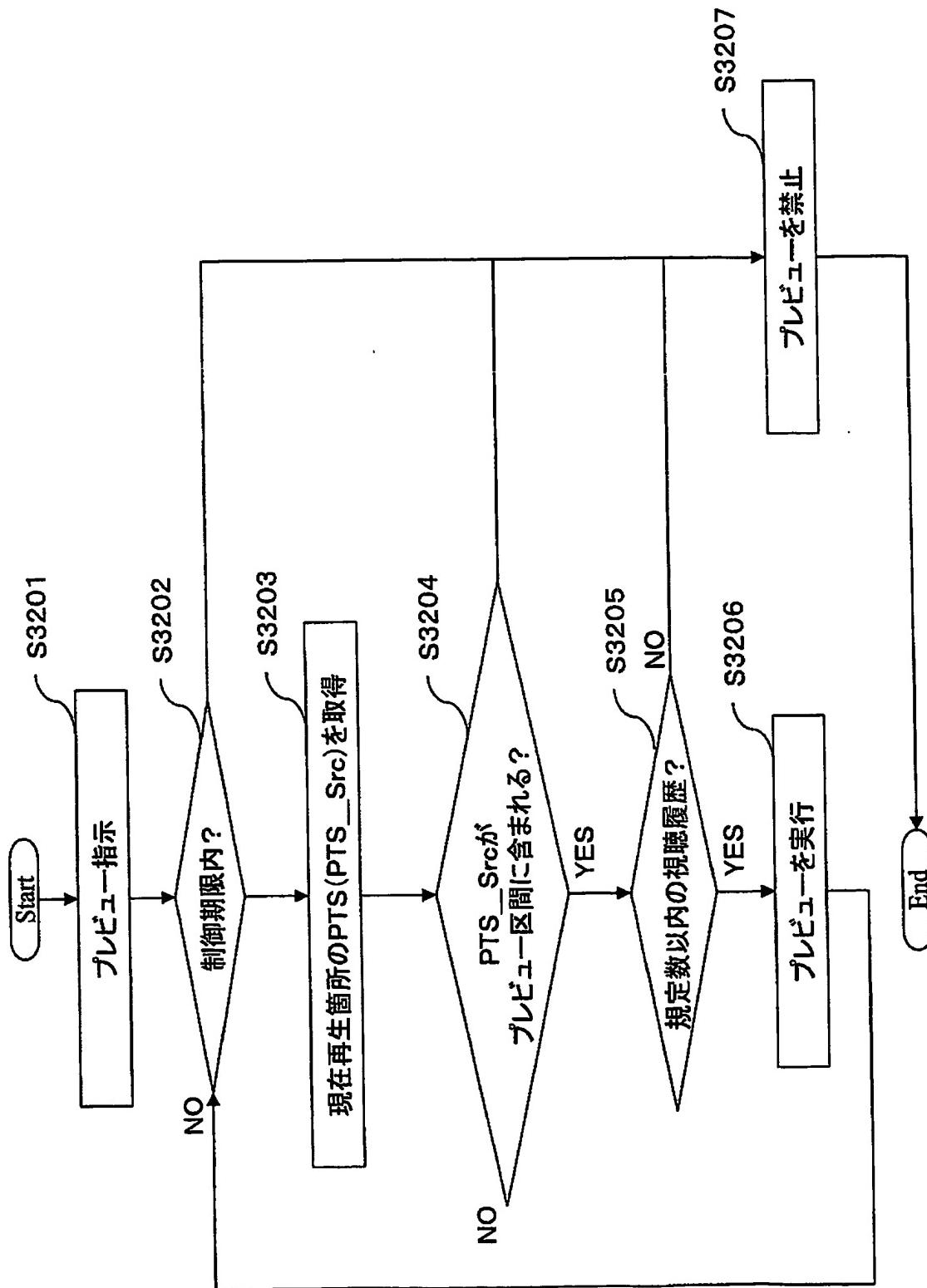
【図30】



【図31】



【図32】



【書類名】要約書

【要約】

【課題】 コンテンツに制御情報を追加することなく、事業者が、ユーザのコンテンツ特定部分の利用をセキュアに制御することが可能なコンテンツ利用制御システムを提供する。

【解決手段】 端末装置にコンテンツを配信するコンテンツ配信サーバと、コンテンツの利用をセキュアに制御する端末装置とから構成されるコンテンツ利用制御システムであって、コンテンツ配信サーバは、時刻情報をコンテンツにセキュアに付加するとともに、時刻情報を用いてコンテンツの特定部分の利用を制御するための利用制御情報をコンテンツとは別データとして生成して端末装置に配信し、端末装置は、コンテンツに付加されたセキュアな時刻情報と利用制御情報を用いて、コンテンツの利用をセキュアに制御する。

【選択図】 図1

## 認定・付加情報

特許出願の番号	特願2003-378574
受付番号	50301848230
書類名	特許願
担当官	第七担当上席 0096
作成日	平成15年11月10日

## &lt;認定情報・付加情報&gt;

【提出日】	平成15年11月 7日
-------	-------------

特願 2003-378574

出願人履歴情報

識別番号 [000005821]

1. 変更年月日 1990年 8月28日

[変更理由] 新規登録

住所 大阪府門真市大字門真1006番地  
氏名 松下電器産業株式会社

**This Page is Inserted by IFW Indexing and Scanning  
Operations and is not part of the Official Record**

## **BEST AVAILABLE IMAGES**

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images include but are not limited to the items checked:

- BLACK BORDERS**
- IMAGE CUT OFF AT TOP, BOTTOM OR SIDES**
- FADED TEXT OR DRAWING**
- BLURRED OR ILLEGIBLE TEXT OR DRAWING**
- SKEWED/SLANTED IMAGES**
- COLOR OR BLACK AND WHITE PHOTOGRAPHS**
- GRAY SCALE DOCUMENTS**
- LINES OR MARKS ON ORIGINAL DOCUMENT**
- REFERENCE(S) OR EXHIBIT(S) SUBMITTED ARE POOR QUALITY**
- OTHER:** \_\_\_\_\_

**IMAGES ARE BEST AVAILABLE COPY.**

**As rescanning these documents will not correct the image problems checked, please do not report these problems to the IFW Image Problem Mailbox.**